WELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales Büro

PCT

INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation 7 : H04K 1/00, H04N 7/167, 7/26	A1	(11) Internationale Veröffentlichungsnummer: **WO 00/51279** (43) Internationales Veröffentlichungsdatum: 31. August 2000 (31.08.00)

(21) Internationales Aktenzeichen: PCT/EP99/09978

(22) Internationales Anmeldedatum: 15. Dezember 1999 (15.12.99)

(30) Prioritätsdaten:
199 07 964.1 24. Februar 1999 (24.02.99) DE

(71) Anmelder *(für alle Bestimmungsstaaten ausser US)*: FRAUNHOFER–GESELLSCHAFT ZUR FÖRDERUNG DER ANGEWANDTEN FORSCHUNG E. V. [DE/DE]; Leonrodstrasse 54, D–80636 München (DE).

(72) Erfinder; und
(75) Erfinder/Anmelder *(nur für US)*: ALLAMANCHE, Eric [DE/DE]; Sulzbacherstrasse 41, D–90489 Nürnberg (DE). HERRE, Jürgen [DE/DE]; Am Eichengarten 11, D–91054 Buckenhof (DE). KOLLER, Jürgen [DE/DE]; St. Johann 6/113, D–91054 Erlangen (DE). RUMP, Niels [DE/DE]; Brückenstrasse 13, D–91056 Erlangen (DE).

(74) Anwalt: SCHOPPE, Fritz; Schoppe, Zimmermann & Stöckeler, Postfach 71 08 67, D–81458 München (DE).

(81) Bestimmungsstaaten: JP, KR, US, europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

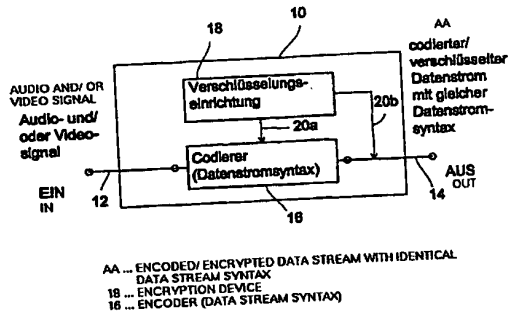
Veröffentlicht
Mit internationalem Recherchenbericht.

(54) Title: DEVICE AND METHOD FOR PRODUCING AN ENCODED AUDIO AND/OR VIDEO DATA STREAM

(54) Bezeichnung: VORRICHTUNG UND VERFAHREN ZUM ERZEUGEN EINES VERSCHLÜSSELTEN AUDIO– UND/ODER VIDEODATENSTROMS

(57) Abstract

The invention relates to a device (10) for producing an encoded data stream which represents an audio and/or video signal. Said device comprises an encoder (16) for encoding an input signal (12) to produce a data stream of a defined data stream syntax as the output signal. Said device further comprises an encryption device (18) which is coupled to the encoder (16) to influence encoding–related data (20a) and/or the output signal (20b) of the encoder in an unequivocally reversible manner on the basis of a code in such a manner that the produced encoded data stream contains useful information that differs from the useful information of a data stream that would be produced by the device without the presence of the encryption device and that the produced encoded data stream has the defined data stream syntax. The invention thus provides a flexible data stream encryption according to which the degree of encryption can be freely selected in such a manner that the user of a decoder who does not possess the code still has a rough idea of the audio and/or video signal that might cause him/her to buy the code to hear or view the audio and/or video signal in its full quality. The encoder–specific encryption and decryption concept can be implemented into already existing encoders/decoders with little effort.



(57) Zusammenfassung

Eine Vorrichtung (10) zum Erzeugen eines verschlüsselten Datenstroms, der ein Audio– und/oder Videosignal darstellt, umfaßt einen Codierer (16) zum Codieren eines Eingangssignals (12), um als Ausgangssignal einen Datenstrom mit einer vordefinierten Datenstromsyntax zu erzeugen. Die Vorrichtung umfaßt ferner eine Verschlusselungseinrichtung (18), die mit dem Codierer (16) gekoppelt ist, um codiererinterne Daten (20a) und/oder das Ausgangssignal (20b) des Codierers auf eindeutig umkehrbare Art und Weise auf der Basis eines Schlüssels zu beeinflussen, derart, daß der erzeugte verschlüsselte Datenstrom Nutzinformationen aufweist, die sich von Nutzinformationen eines Datenstroms unterscheiden, der durch die Vorrichtung ohne Vorhandensein der Verschlüsselungseinrichtung erzeugt werden würde, und daß der erzeugte verschlüsselte Datenstrom die vordefinierte Datenstromsyntax aufweist. Damit wird eine flexible Datenstromverschlüsselung erreicht, wobei der Grad der Verschlüsselung beliebig einstellbar ist, derart, daß ein Besitzer eines Decodierers, der nicht im Besitz des Schlüssels ist, noch einen groben Eindruck des Audio– und/oder Videosignals erhält, was ihn vielleicht dazu veranlaßt, den Schlüssel zu kaufen, um das Audio– und/oder Videosignal in voller Qualität hören bzw. betrachten zu können. Das codiererspezifische Verschlüsselungs– bzw. Entschlüsselungskonzept kann mit geringem Aufwand in bereits bestehende Codierer/Decodierer implementiert werden.

LEDIGLICH ZUR INFORMATION

Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

AL	Albanien
AM	Armenien
AT	Österreich
AU	Australien
AZ	Aserbaidschan
BA	Bosnien-Herzegowina
BB	Barbados
BE	Belgien
BF	Burkina Faso
BG	Bulgarien
BJ	Benin
BR	Brasilien
BY	Belarus
CA	Kanada
CF	Zentralafrikanische Republik
CG	Kongo
CH	Schweiz
CI	Côte d'Ivoire
CM	Kamerun
CN	China
CU	Kuba
CZ	Tschechische Republik
DE	Deutschland
DK	Dänemark
EE	Estland
ES	Spanien
FI	Finnland
FR	Frankreich
GA	Gabun
GB	Vereinigtes Königreich
GE	Georgien
GH	Ghana
GN	Guinea
GR	Griechenland
HU	Ungarn
IE	Irland
IL	Israel
IS	Island
IT	Italien
JP	Japan
KE	Kenia
KG	Kirgisistan
KP	Demokratische Volksrepublik Korea
KR	Republik Korea
KZ	Kasachstan
LC	St. Lucia
LI	Liechtenstein
LK	Sri Lanka
LR	Liberia
LS	Lesotho
LT	Litauen
LU	Luxemburg
LV	Lettland
MC	Monaco
MD	Republik Moldau
MG	Madagaskar
MK	Die ehemalige jugoslawische Republik Mazedonien
ML	Mali
MN	Mongolei
MR	Mauretanien
MW	Malawi
MX	Mexiko
NE	Niger
NL	Niederlande
NO	Norwegen
NZ	Neuseeland
PL	Polen
PT	Portugal
RO	Rumänien
RU	Russische Föderation
SD	Sudan
SE	Schweden
SG	Singapur
SI	Slowenien
SK	Slowakei
SN	Senegal
SZ	Swasiland
TD	Tschad
TG	Togo
TJ	Tadschikistan
TM	Turkmenistan
TR	Türkei
TT	Trinidad und Tobago
UA	Ukraine
UG	Uganda
US	Vereinigte Staaten von Amerika
UZ	Usbekistan
VN	Vietnam
YU	Jugoslawien
ZW	Zimbabwe

VORRICHTUNG UND VERFAHREN ZUM ERZEUGEN EINES VERSCHLÜSSELTEN AUDIO- UND/ODER VIDEODATENSTROMS

Beschreibung

Die vorliegende Erfindung bezieht sich auf die Ver- bzw. Entschlüsselung von Audio- und/oder Videosignalen und insbesondere auf ein flexibles Konzept zum kundenselektiven Bereitstellen von Audio- und/oder Videosignalen.

Mit der breiten Verfügbarkeit des Internets in Verbindung mit gehörangepaßten Audiocodierverfahren wurde eine einfache weltweite Verteilung hochwertiger Audiosignale möglich. Dies hat insbesondere weltweit auch zu einer Welle der Musik-Piraterie geführt, bei der Personen beispielsweise gekaufte CD-Musik gemäß dem Standard MPEG Layer-3 (MP3) codieren und illegal auf das World Wide Web (WWW) legen. Schätzungen gehen davon aus, daß die Anzahl der so ausgetauschten Musikstücke bei etwa 10 Millionen Downloads pro Tag liegt, ohne daß die Halter der dazu gehörigen Urheber- bzw. Lizenzrechte dies autorisiert haben oder eine entsprechende Abgabe erhalten. Dies hat zu großer Besorgnis in der Musikindustrie geführt.

Insbesondere bestehen heutzutage mehrere Randbedingungen, wenn die Musikverteilungssituation betrachtet wird. Zum einen existiert ein weit verbreitetes Know-How bezüglich der Audiokompressionstechnologie, was sich beispielsweise in dem Standard MPEG Layer-3 (MP3) manifestiert hat. Weiterhin laufen Softwarecodierer, Softwaredecodierer und Abspielgeräte für MP3 (beispielsweise mp3enc, l3enc, WinPlay3) und andere Formate auf einer Vielzahl von Betriebssystemen, einschließlich des Windows-Betriebssystems. Außerdem existieren viele Internetstellen, die MP3-Musik anbieten, die oftmals ohne Autorisierung dort plaziert worden ist.

Neben den Software-Codierern und -Decodierern existieren auch Hardware-Abspielgeräte, wie z. B. MPLayer3, MP-Man, Rio, usw., die in der Lage sind, MP3-Stücke abzuspielen, die entweder von einer CD codiert worden sind, oder die Dateien sind, die von dem Internet heruntergeladen worden sind. Diese Abspielgeräte haben bisher keinerlei implementierte Schutztechniken, um Urheber- oder Lizenzrechten Geltung zu verschaffen. Darüberhinaus existieren Geräte zum Beschreiben von CD-ROMs, die Audio-CDs und MP3-CD-ROMs beschreiben können. Diese Geräte werden mittlerweile zu Preisen angeboten, die zu einer breiten Verfügbarkeit geführt haben. Ferner sind die Preise für hochvolumige Festplatten gefallen, weshalb die allermeisten Internet-Teilnehmer über nahezu unbegrenzte Speichermöglichkeiten verfügen. Schließlich sei noch auf die Tendenz hingewiesen, daß die Übertragungskosten für Dateien immer mehr abnehmen.

Obwohl bei den beschriebenen Hardware-Abspielgeräten noch keine Schutztechniken implementiert sind, existieren dennoch mehrere Techniken zum Schützen von Audio- und/oder Video-Daten (d. h. Multimediadaten, von denen das Multimedia Protection Protocol MMP genannt sei. Diese Technologie stellt eine sogenannte "Secure Envelope"- Technik dar.

Die DE 196 25 625 C1 beschreibt eine solche Technik zur Verschlüsselung und Entschlüsselung von Multimediadaten. Dabei werden nach einem Audio- oder Videostandard codierte Daten zumindest teilweise mittels z. B. eines DES-Verschlüsselungsverfahrens (DES = Data Encryption Standard = Datenverschlüsselungsstandard) verschlüsselt und in einen Nutzdatenblock geschrieben. Der Nutzdatenblock wird mit einem Bestimmungsdatenblock versehen, der neben einer Vielzahl weiterer Informationen auch Informationen bezüglich des bei der Verschlüsselung verwendeten Verschlüsselungsalgorithmus sowie eines dazu benötigten Schlüssels umfaßt. Der Schlüssel umfaßt dabei Benutzerinformationen, derart, daß nur ein spezieller Benutzer, der zum Abspielen eines Multimediastücks beispielsweise durch Kauf oder Lizenzierung berechtigt ist,

das Stück entschlüsseln kann. Ein Abspielgerät, das nicht den korrekten Schlüssel hat, wird, sobald es auf die verschlüsselten Multimediadaten trifft, den Betrieb einstellen. Damit ist das Ziel erreicht, daß nur der Benutzer, der autorisiert ist, ein Multimediastück abspielen kann. Diese Secure Envelope Technik stellt somit ein zweistufiges Verfahren dar, bei dem ein Multimediastück zunächst codiert wird, um eine erhebliche Datenkompression zu erreichen, und bei dem dann ein kryptographischer Algorithmus eingesetzt wird, um das codierte Multimediastück gegen unerlaubte Angreifer zu verteidigen.

Für Anwendungen, die keinen solchen Maximalschutz erfordern, ist das beschriebene Konzept darin nachteilig, daß es relativ aufwendig werden kann und wesentliche Modifikationen an Abspielgeräten erforderlich macht, um den Bestimmungsdatenblock verarbeiten zu können. Die Abspielgeräte, die letztendlich Massenprodukte im Consumer-Bereich sind, und daher preisgünstig angeboten werden müssen, sollten jedoch wenn möglich überhaupt nicht verändert werden müssen, um auch geschützte Multimediastücke abspielen zu können. Damit bleibt festzustellen, daß das bekannte Verschlüsselungskonzept zwar einen maximalen Schutz und eine hohe Verschlüsselungsflexibilität durch entsprechendes Gestalten des Anfangsblocks möglich macht, daß jedoch ebenso deutliche Veränderungen an Abspielgeräten erforderlich sind, um verschlüsselte Dateien wieder entschlüsseln bzw. überhaupt einlesen zu können.

Die Aufgabe der vorliegenden Erfindung besteht darin, ein anderes Konzept zum Ver- bzw. Entschlüsseln von Audio- und/oder Videosignalen zu schaffen.

Diese Aufgabe wird durch eine Vorrichtung zum Erzeugen eines verschlüsselten Datenstroms nach Patentanspruch 1, 17 oder 18 durch eine Vorrichtung zum Erzeugen eines entschlüsselten Datenstroms nach Patentanspruch 19 oder 23, durch ein Verfahren zum Erzeugen eines verschlüsselten Datenstroms nach Patentanspruch 29 und durch ein Verfahren zum Erzeugen eines

entschlüsselten Datenstroms nach Patentanspruch 30 gelöst.

Der vorliegenden Erfindung liegt die Erkenntnis zugrunde, daß im Sinne einer flexiblen Ver- bzw. Entschlüsselung vom "Secure Envelope"-Konzept abgegangen werden kann, und daß ein sogenanntes "Soft-Envelope"-Konzept dazu dienen kann, mit sehr begrenzten Änderungen an bereits bestehenden Abspielgeräten auszukommen. Dies hat den Vorteil, daß die Investitionen für Neuentwicklungen, die zu einer ausreichenden Verschlüsselung benötigt werden, gering gehalten werden können. Dies wird erreicht, indem nicht ein Allzweck-Verschlüsselungsverfahren eingesetzt wird, das für jede beliebige Art von Daten anwendbar ist, sondern daß eine Spezialzweck-Verschlüsselung eingesetzt wird, die auf den speziellen Codierer bzw. Decodierer angepaßt ist. Insbesondere bei hochkomprimierenden Codierverfahren, wie z. B. Verfahren nach dem Standard MPEG-1 und MPEG-2 einschließlich MPEG-2 AAC, werden bereits so viel Veränderungen an den zu komprimierenden Daten durchgeführt, daß bereits kleine Veränderungen an codiererinternen Daten und/oder an den Ausgangsdaten des Codierers genügen, um zumindest eine (reversible) Qualitätsverschlechterung des Audio- und/oder Videosignals am Ausgang eines Decodierers, der keine Kenntnis über die im Codierer eingeführten Veränderungen hat, einzuführen, wodurch eine "weiche" Verschlüsselung erreicht ist. Erfindungsgemäß werden nur solche Änderungen durchgeführt, die die Datenstromsyntax des Codierers nicht verändern. Damit kann ein erfindungsgemäß verschlüsselter Datenstrom ohne weiteres von einem Decodierer eingelesen und decodiert werden. Das decodierte Ausgangssignal hat dann bei Nichtkenntnis der Art und Weise der Verschlüsselung, d. h. bei Nichtkenntnis des Schlüssels, eine geringere Qualität.

Ein wesentlicher Vorteil des erfindungsgemäßen Konzepts besteht demnach darin, daß durch die Art und Weise des Eingriffs in die codiererinternen Daten und/oder in die Ausgangsdaten des Codierers eine sehr leichte Verschlüsselung genauso implementiert werden kann, wie eine sehr starke

Verschlüsselung, bei der das Ausgangssignal eines nicht-autorisierten Decodierers kaum mehr Ähnlichkeit mit dem ursprünglichen Signal am Eingang des Codierers hat. Ein wesentlicher Vorteil der vorliegenden Erfindung besteht nun jedoch im Gegensatz zu Allzweck-Verschlüsselungsverfahren darin, daß die Vorrichtung zum Erzeugen eines verschlüsselten Datenstroms nicht die durch den Codierer festgelegte Datenstromsyntax verändert. Damit sind keine wesentlichen Modifikationen an einem Decodierer, der, wie es bereits erwähnt wurde, ein Massenartikel ist und preisgünstig und billig sein muß, erforderlich.

Gemäß einem bevorzugten Ausführungsbeispiel der vorliegenden Erfindung wird die Beeinflussung der codiererinternen Daten und/oder der Ausgangsdaten des Codierers durch eine Verschlüsselungseinrichtung lediglich so intensiv ausgeführt, daß ein nicht-autorisierter Decodierer noch Ausgangssignale mit einer gewissen Audio- und/oder Videoqualität liefert. Damit kann ein Benutzer eines nicht-autorisierten Decodierers zumindest einen groben Eindruck der verschlüsselten Musik gewinnen, was ihn unter Umständen zum Kauf einer autorisierten Version, d. h. des Schlüssels, bewegt, um die Beeinflussungen der Daten, die in der Vorrichtung zum Erzeugen des verschlüsselten Datenstroms ausgeführt worden sind, wieder in einer Vorrichtung zum Erzeugen eines entschlüsselten Datenstroms rückgängig zu machen, um volle Audio- und/oder Videoqualität zur erlangen.

Ein weiterer wesentlicher Vorteil der vorliegenden Erfindung besteht darin, daß es möglich ist, Audio- und/oder Videosignale so zu verschlüsseln, daß der verschlüsselte Datenstrom exakt die gleiche Länge hat wie der nicht-verschlüsselte lediglich codierte Datenstrom. Wenn ein Codierer so implementiert ist, daß er eine Datenrate liefert, die beispielsweise genau der maximalen Datenrate einer ISDN-Telephonleitung entspricht, so ist eine Echtzeit-Übertragung des codierten nicht-verschlüsselten Datenstroms möglich. Würde ein Verschlüsselungsverfahren einen längeren Datenstrom erzeugen,

würde eine Echtzeitübertragung über diese ISDN-Leitung nicht möglich sein.

Die vorliegende Erfindung liefert daher ein Verschlüsselungs- bzw. Entschlüsselungskonzept, bei dem an keiner Stelle die durch den Codierer festgelegte Datenstromsyntax verändert wird. Ein solches Verschlüsselungs- bzw. Entschlüsselungskonzept liefert aus diesem Grund eine maximale Flexibilität, da ein Decodierer einen verschlüsselten Datenstrom immer aufgrund der beibehaltenen Datenstromsyntax decodieren kann. Abhängig von der Datenbeeinflussung in der Entschlüsselungseinrichtung kann nun jedoch eine sehr leichte oder eine sehr starke Verschlüsselung erreicht werden, derart, daß ein nicht-autorisierter Hörer durch seinen Decodierer noch einen relativ guten Eindruck der verschlüsselten Daten oder aber einen sehr schlechten bzw. überhaupt keinen Eindruck mehr von den verschlüsselten Daten erhalten kann. Aufgrund der Tatsache, daß die durch den Codierer vordefinierte Datenstromsyntax durch die Verschlüsselung nicht angetastet wird, sind keine besonders großen Änderungen an bestehenden Abspielgeräten, d. h. Decodierern nötig, um das erfindungsgemäße Konzept implementieren zu können. Diese Eigenschaft ist wesentlich, da ein Multimediadaten-Schutzkonzept, d. h. ein Schutzkonzept für Audio- und/oder Videodaten, nur dann am Markt Akzeptanz finden wird, wenn es ohne wesentliche Kosten implementiert werden kann, und wenn es einfach zu bedienen ist.

Schließlich ist das erfindungsgemäße Konzept werbewirksam, da sämtliche bestehenden Decodierer zum Decodieren verwendet werden können, weshalb Benutzer von bestehenden Decodierern verschlüsselte Stücke - mit verminderter Qualität - anhören können und damit unter Umständen zum Kauf des Schlüssels bzw. zum Kauf/zur Lizensierung auch einer erfindungsgemäßen Vorrichtung zum Erzeugen eines entschlüsselten Datenstroms motiviert werden, um die volle Audio- und/oder Videoqualität genießen zu können.

Bevorzugte Ausführungsbeispiele der vorliegenden Erfindung werden nachfolgend bezugnehmend auf die beiliegenden Zeichnungen detailliert erläutert. Es zeigen:

Fig. 1 ein schematisches Blockdiagramm einer erfindungsgemäßen Vorrichtung zum Erzeugen eines verschlüsselten Datenstroms aus einem Audio- und/oder Videosignal;

Fig. 2 ein schematisches Blockdiagramm einer erfindungsgemäßen Vorrichtung zum Erzeugen eines Audio- und/oder Videosignals als entschlüsselter Datenstrom;

Fig. 3 ein Ausführungsbeispiel einer erfindungsgemäßen Vorrichtung zum Erzeugen eines verschlüsselten Datenstroms, die einen Audiocodierer nach dem Standard MPEG Layer-3 oder MPEG-2 AAC aufweist;

Fig. 4 eine Vorrichtung zum Erzeugen eines verschlüsselten Datenstroms gemäß einem weiteren Ausführungsbeispiel der vorliegenden Erfindung, die einen Audiocodierer nach dem Standard MPEG Layer-3 oder dem Standard MPEG-2 AAC aufweist;

Fig. 5 eine Vorrichtung zum Erzeugen eines entschlüsselten Audio- und/oder Videosignals gemäß einem weiteren Ausführungsbeispiel der vorliegenden Erfindung, die zu der Vorrichtung zum Erzeugen eines verschlüsselten Datenstroms von Fig. 3 komplementär ist;

Fig. 6 eine Vorrichtung zum Erzeugen eines entschlüsselten Audio- und/oder Videosignals gemäß einem weiteren Ausführungsbeispiel der vorliegenden Erfindung, die zu der Vorrichtung zum Erzeugen eines verschlüsselten Datenstroms von Fig. 4 komplementär ist;

Fig. 7 eine Vorrichtung zum Erzeugen eines verschlüsselten Datenstroms gemäß einem weiteren Ausführungsbei-

spiel der vorliegenden Erfindung, um einen mit einem ersten Schlüssel verschlüsselten Datenstrom in einen mit einem zweiten Schlüssel verschlüsselten Datenstrom umzusetzen;

Fig. 8 eine Vorrichtung zum Erzeugen eines verschlüsselten Datenstroms gemäß einem weiteren Ausführungsbeispiel der vorliegenden Erfindung, um einen codierten/nicht-verschlüsselten Datenstrom in einen codierten/verschlüsselten Datenstrom umzuwandeln;

Fig. 9 eine Vorrichtung zum Erzeugen eines entschlüsselten Datenstroms gemäß einem weiteren Ausführungsbeispiel der vorliegenden Erfindung, um einen codierten/verschlüsselten Datenstrom in einen codierten/nicht-verschlüsselten Datenstrom umzuwandeln;

Fig. 10 ein schematisches Blockschaltbild eines bekannten Audiocodierers z. B. nach dem Standard MPEG Layer-3 oder nach dem Standard MPEG-2 AAC; und

Fig. 11 ein schematisches Blockschaltbild eines bekannten Audio-Decodierers nach dem Standard MPEG Layer-3 oder nach dem Standard MPEG-2 AAC.

Fig. 1 zeigt ein allgemeines Blockschaltbild einer erfindungsgemäßen Vorrichtung 10 zum Erzeugen eines verschlüsselten Datenstroms, der ein Audio- und/oder Videosignal darstellt. Die Vorrichtung 10 umfaßt einen Eingang 12 und einen Ausgang 14. Zwischen den Eingang 12 und den Ausgang 14 ist ein Codierer 16 geschaltet, der mit einer Verschlüsselungseinrichtung 18 gekoppelt ist, um am Ausgang der Vorrichtung 10 zum Erzeugen eines verschlüsselten Datenstroms einen verschlüsselten Datenstrom zu liefern, der die gleiche Datenstromsyntax aufweist, wie sie der Codierer 16 gewissermaßen festlegt bzw. fordert.

Die Verschlüsselungseinrichtung 18 und der Codierer 16 sind

derart gekoppelt, daß die Verschlüsselungseinrichtung 18 codiererinterne Daten (Zweig 20a) und/oder Ausgangsdaten des Codierers (Zweig 20b) beeinflußt, jedoch lediglich derart beeinflußt, daß sich die Datenstromsyntax des Datenstroms am Ausgang 14 der Vorrichtung 10 zum Erzeugen eines verschlüsselten Datenstroms nicht von der durch den Codierer 16 bestimmten Datenstromsyntax unterscheidet. Insbesondere umfaßt die Beeinflussung durch die Verschlüsselungseinrichtung 18 eine Veränderung der codiererinternen Daten 20a und/oder der Ausgangsdaten des Codierers 20b auf eine eindeutig umkehrbare Art und Weise auf der Basis eines Schlüssels, was dazu führt, daß sich der an dem Ausgang 14 erzeugte verschlüsselte Datenstrom bezüglich seiner Nutzinformationen von den Nutzinformationen eines Datenstroms unterscheidet, der durch den Codierer 16 (bzw. durch die Vorrichtung 10) erzeugt werden würde, wenn derselbe keiner Beeinflussung durch die Verschlüsselungseinrichtung 18 unterzogen wäre.

Wie es bereits erwähnt worden ist, ist der Codierer 16 gemäß einem bevorzugten Ausführungsbeispiel der vorliegenden Erfindung als Audiocodierer gemäß dem Standard MPEG Layer-3 oder gemäß dem Standard MPEG-2 AAC ausgeführt. Derselbe könnte jedoch ebenfalls ein Audiocodierer ohne Entropiecodierung, wie z. B. nach dem Standard MPEG Layer-2 sein. Darüberhinaus könnte der Codierer 16 ebenfalls ein Codierer für Sprachsignale sein, der keine Codierung im Frequenzbereich durchführt, sondern eine Codierung im Zeitbereich beispielsweise unter Verwendung von Prädiktions- oder Vektorquantisierungstechniken durchführt. Der Codierer 16 könnte selbstverständlich auch ein Videocodierer sein, der Videoeingangsdaten komprimiert, um eine Übertragung derselben über Bandbreiten-begrenzte Übertragungskanäle zu ermöglichen.

Der Codierer 16 kann somit ein beliebiger Codierer sein, der Eingangsdaten in denselben gemäß festgelegter Vorschriften in codierte Ausgangsdaten umformt, wobei die Datenstromsyntax der Ausgangsdaten durch den Codierer definiert ist. Üblicherweise existiert zu jedem Codierer ein Decodierer, der-

art, daß der codierte Datenstrom wieder decodiert werden kann. Dies bedeutet jedoch weiterhin, daß jeder Codierer einen Datenstrom mit einer vordefinierten Datenstromsyntax erzeugt, die schon allein deshalb vordefiniert sein muß, damit ein Decodierer, der zu dem Codierer im wesentlichen komplementär ist, den codierten Datenstrom wieder decodieren kann. Dies ist jedoch nur möglich, wenn der Decodierer die Datenstromsyntax des codierten Datenstroms verstehen bzw. interpretieren kann. Daher kann jedem beliebigen Codierer, zu dem ein Decodierer existiert, eine vordefinierte Datenstromsyntax zugeschrieben werden.

Fig. 2 zeigt ein schematisches Blockschaltbild einer erfindungsgemäßen Vorrichtung 30 zum Erzeugen eines entschlüsselten Datenstroms. Dieselbe umfaßt einen Eingang 32 und einen Ausgang 34. Zwischen dem Eingang 32 und dem Ausgang 34 ist ein Decodierer 36 geschaltet, der für eine vordefinierte Datenstromsyntax ausgerichtet ist, die durch den Codierer 16 (Fig. 1) bestimmt wird, und die erfindungsgemäß durch die Verschlüsselungseinrichtung 18 (Fig. 1) nicht angetastet wird, derart, daß der Datenstrom am Ausgang 14 der Vorrichtung 10 zum Erzeugen eines verschlüsselten Datenstroms die gleiche Datenstromsyntax hat wie der Datenstrom am Eingang 32 der Vorrichtung 30 zum Erzeugen eines entschlüsselten Datenstroms.

Die Vorrichtung 30 zum Erzeugen eines entschlüsselten Datenstroms ist im wesentlichen komplementär zu der Vorrichtung zum Erzeugen eines verschlüsselten Datenstroms 10, derart, daß sie neben dem Decodierer 36 auch eine Entschlüsselungseinrichtung 38 aufweist, die wiederum mit dem Decodierer 36 gekoppelt ist, um Eingangsdaten in den Decodierer 36 (Zweig 40a) bzw. Decodierer-interne Daten (Zweig 40b) auf der Basis des beim Verschlüsseln verwendeten Schlüssels zu beeinflussen, derart, daß die durch die Vorrichtung 10 zum Erzeugen eines verschlüsselten Datenstroms eingeführten Veränderungen, die eindeutig umkehrbare Veränderungen waren, wieder rückgängig gemacht werden, um am Ausgang 34 einen decodier-

ten und unverschlüsselten Datenstrom zu erhalten.

Am Beispiel eines Audiocodierers sei das erfindungsgemäße Konzept anhand der Fig. 1 und 2 veranschaulicht. Am Eingang 12 der Vorrichtung 10 zum Erzeugen eines verschlüsselten Datenstroms würde in diesem Fall ein zeitdiskretes Audiosignal anliegen, das durch den Codierer 16 codiert wird, und das am Ausgang 14 der Vorrichtung zum Erzeugen eines verschlüsselten Datenstroms als Bitstrom ausgegeben wird, der dieselbe Bitstromsyntax hat, wie sie für den Codierer 16 vordefiniert ist, der jedoch aufgrund der Verschlüsselungseinrichtung 18 und insbesondere aufgrund der Beeinflussung der Daten über die Zweige 20a und 20b verschlüsselt worden ist. Der verschlüsselte codierte Bitstrom wird in den Eingang 32 der Vorrichtung 30 zum Erzeugen eines entschlüsselten Datenstroms eingegeben, und durch den Audio-Decodierer 36 wieder decodiert, um am Ausgang 34 wieder das zeitdiskrete Audiosignal zu erhalten. Ist die Vorrichtung 30 zum Erzeugen eines entschlüsselten Datenstroms autorisiert, d. h. kennt sie den von der Verschlüsselungseinrichtung 18 verwendeten Schlüssel, so wird sie die Verschlüsselungen über die Zweige 40a bis 40c wieder rückgängig machen, derart, daß das zeitdiskrete Audiosignal am Ausgang 34 der Vorrichtung 30 zum Erzeugen eines entschlüsselten Datenstroms ein Audiosignal mit voller Audioqualität ist. Ist die Vorrichtung 30 dagegen nicht autorisiert, d. h. kennt sie nicht den verwendeten Schlüssel, so wird das zeitdiskrete Audiosignal am Ausgang 34 ein Audiosignal sein, das sich je nach Anwendung mehr oder weniger von dem Audiosignal am Eingang 12 der Vorrichtung 10 unterscheiden wird. Ist die Datenbeeinflussung durch die Verschlüsselungseinrichtung nur begrenzt gewesen, so wird das zeitdiskrete Audiosignal am Ausgang 34 der Vorrichtung 30 zum Erzeugen eines entschlüsselten Datenstroms dem nicht-autorisierten Benutzer noch einen gewissen Höreindruck liefern, der ihn vielleicht dazu motiviert, sich autorisieren zu lassen, d. h. den Schlüssel, den die Verschlüsselungseinrichtung 18 angewendet hat, zu kaufen, um in den vollen Genuß zu kommen.

Bevor anhand der Fig. 3 bis 9 auf mehrere bevorzugte Ausführungsbeispiele der vorliegenden Erfindung eingegangen wird, werden zunächst anhand von Fig. 10 ein bekanntes Codierererkonzept und anhand von Fig. 11 ein bekanntes Decodiererkonzept beschrieben.

Fig. 10 stellt ein Blockschaltbild für einen bekannten Audiocodierer dar, der beispielsweise nach dem Standard ISO/IEC 13818-7 (MPEG-2 AAC) ausgeführt ist. Derselbe umfaßt einen Audioeingang 200 und einen Bitstromausgang 202. Ein zeitdiskretes Audiosignal am Audioeingang 200 wird in eine Analyse-Filterbank 204 eingespeist, um in den Frequenzbereich abgebildet zu werden, derart, daß sich am Ausgang der Analyse-Filterbank ein Satz von Spektralwerten ergibt, die das Kurzzeitspektrum des Audiosignals am Eingang 200 darstellen, d. h. ein Block von zeitdiskreten Audiosignal-Abtastwerten wird durch die Analyse-Filterbank 204 in einen Block von Spektralwerten, d. h. in eine spektrale Darstellung, umgesetzt. Diese Spektralwerte werden in einem mit Quantisierung bezeichneten Block 206 unter Berücksichtigung eines psychoakustischen Modells 208 quantisiert, derart, daß eine möglichst bitsparende Quantisierung erreicht wird, daß jedoch das eingeführte Quantisierungsrauschen unter der Maskierungsschwelle des Audiosignals am Eingang 200 liegt, so daß es unhörbar bleibt.

Es handelt sich somit um eine verlustbehaftete Quantisierung (allgemeiner gesagt verlustbehaftete Codierung), die jedoch zu keinen störenden Höreinflüssen führt. Die quantisierten Spektralwerte 206 werden, um eine weitere Datenkompression zu erreichen, in einem Block 210 einer Entropie-Codierung unterzogen. Die Entropie-codierten quantisierten Spektralwerte werden schließlich einem Bitstrom-Multiplexer 212 zugeführt, der gemäß der vordefinierten Codierersyntax den Entropie-codierten quantisierten Spektralwerten die entsprechenden Seiteninformationen hinzufügt, derart, daß an dem Bitstromausgang 202 ein codierter Bitstrom ausgegeben wird,

der als Nutzinformationen Hauptinformationen in Form der Entropie-codierten quantisierten Spektralwerte und Nebeninformationen in Form von Seiteninformationen, wie z. B. Skalenfaktoren, usw., aufweist. Bezüglich näherer Details zu den einzelnen Codiererblöcken, die in Fig. 10 gezeigt sind, bzw. zu weiteren dort nicht gezeigten Blöcken, wie z. B. Blöcken zur Verarbeitung von Stereosignalen, etc., sei auf den Standard ISO/IEC 13818-7 (MPEG-2 AAC) verwiesen. Dieser Standard umfaßt ferner eine detaillierte Darstellung der im Block 210 ausgeführten Entropie-Codierung. Es sei darauf hingewiesen, daß das erfindungsgemäße Konzept ebenfalls auf einen Codierer ohne Entropie-Codierung (MPEG Layer-1 und Layer-2), und allgemein auf jeglichen Codierer angewendet werden kann, der einen codierten Datenstrom mit einer vordefinierten Datenstromsyntax erzeugt. Für die vorliegende Erfindung ist es insbesondere nicht relevant, wie die Umsetzung der zeitlichen Daten in die spektralen Daten bewirkt wird, dieselbe ist daher auf auf die sogenannten Subbandcodierer (z. B. MPEG-1) anwendbar.

Fig. 11 zeigt einen zu Fig. 10 komplementären Decodierer, der ebenfalls nach dem AAC-Standard ausgeführt sein kann. Derselbe umfaßt einen Bitstromeingang 220, der mit einem Bitstrom-Demultiplexer 222 gekoppelt ist, der eine zum Bitstrom-Multiplexer 212 (Fig. 10) komplementäre Demultiplex-Operation durchführt, um unter anderem Entropie-codierte quantisierte Spektralwerte in eine Entropie-Decodierungseinrichtung 224 einzuspeisen, die die im Block 210 (Fig. 10) eingeführte Entropie-Codierung wieder rückgängig macht. Die nun nur noch quantisierten Spektralwerte werden in einem Block 226 einer inversen Quantisierung unterzogen, die komplementär zu der im Block 206 durchgeführten Operation ist. Die nun wieder requantisierten Spektralwerte werden in einer Synthese-Filterbank 228 wieder von der spektralen Darstellung in die zeitliche Darstellung umgesetzt, um an einem Audioausgang 230 ein zeitdiskretes Audiosignal zu erhalten.

Bezugnehmend auf Fig. 1 wurde davon gesprochen, daß die er-

findungsgemäße Vorrichtung zum Erzeugen eines verschlüsselten Datenstroms, wie sie in Fig. 1 schematisch dargestellt ist, über den Zweig 20a codiererinterne Daten beeinflussen kann und/oder über den Zweig 20b Ausgangsdaten des Codierers 16 beeinflussen kann. Dies sei anhand des bekannten Codierers, der in Fig. 10 beispielhaft dargestellt ist, erläutert. Eingangsdaten für den Codierer sind zeitdiskrete Audiosignale.

Der in Fig. 1 gezeigte Zweig 20a bezieht sich auf codiererinterne Daten. Aus Fig. 10 ist ersichtlich, daß Codierer aus einer Vielzahl von aufeinanderfolgenden Blöcken zusammengesetzt werden können, wobei prinzipiell jegliche Ein- bzw. Ausgangsdaten eines Blocks auf eindeutig umkehrbare Art und Weise beeinflußt werden können, um eine Verschlüsselung zu erreichen, ohne die Bitstromsyntax zu verändern. Genauso könnten Steuerdaten, wie z. B. Steuerdaten für die Analyse-Filterbank 204, für die Quantisierung 206, für die Entropie-Codierung 210, etc. beeinflußt werden. Codiererinterne Daten sind daher nicht nur die eigentlichen Nutzdaten, d. h. die mehr oder weniger verarbeiteten Spektralwerte, sondern auch die Steuerdaten, die üblicherweise als Seiteninformationen in dem codierten Bitstrom auftreten. Schließlich können auch Ausgangsdaten des Codierers, d. h. am Ausgang des Bitstrom-Multiplexers 212, beeinflußt werden, ohne die Bitstromsyntax zu ändern. Im einfachsten Fall könnten beispielsweise Entropie-codierte Wörter umsortiert, d. h. verwürfelt oder gescrambelt, werden. Selbstverständlich könnten die Codewörter auch bereits direkt vor dem Bitstrom-Multiplexer auf der Basis eines Schlüssels auf eindeutig umkehrbare Art und Weise verwürfelt werden, woraus deutlich wird, daß es im Prinzip unerheblich ist, ob Eingangsdaten des Codierers von Fig. 10, codiererinterne Daten oder Ausgangsdaten des Codierers durch die Verschlüsselungseinrichtung 18 (Fig. 1) beeinflußt werden.

An dieser Stelle sei darauf hingewiesen, daß eine Verwürfelung einzelner Bits von Entropie-Codewörtern zu einer Zer-

störung der Datenstromsyntax führen kann, da beispielsweise Huffman-Codewörter eine unterschiedliche Länge haben und ein Entropie-Decodierer, der mit bitweise verwürfelten Codewörtern konfrontiert wird, sehr wahrscheinlich nicht mehr korrekt arbeiten kann, da er nicht in der Lage ist, den korrekten Anfang bzw. das korrekte Ende eines Codeworts zu finden, weil die Datenstromsyntax innerhalb der Codewörter gestört ist.

Im nachfolgenden wird auf Fig. 3 Bezug genommen, um ein bevorzugtes Ausführungsbeispiel der vorliegenden Erfindung für die Vorrichtung 10 zum Erzeugen eines verschlüsselten Datenstroms zu erläutern. In Fig. 3 sowie in den folgenden Figuren haben gleiche Elemente gleiche Bezugszeichen. Insbesondere haben die bezüglich Fig. 10 und Fig. 11 beschriebenen Blöcke die gleichen Bezugszeichen.

Fig. 3 zeigt ein bevorzugtes Ausführungsbeispiel, bei dem die Verschlüsselungseinrichtung 18 lediglich codiererinterne Daten, d. h. Entropie-codierte quantisierte Spektralwerte beeinflußt. Sie vollführt dies unter Verwendung einer Verwürfelungs- oder "Scrambling"-Einheit, derart, daß Entropie-codierte quantisierte Spektralwerte, die durch Codewörter dargestellt werden, in Abhängigkeit von einem Schlüssel k z. B. umpositioniert, d. h. umsortiert, werden. So könnten beispielsweise immer zwei benachbarte Codewörter vertauscht werden. Dies würde im decodierten Audiosignal zu deutlichen Qualitätseinbußen führen, jedoch nicht dazu, daß ein Benutzer überhaupt keinen Eindruck von dem Audiosignal mehr bekommen würde. Die Verwürfelungseinheit 180 könnte jedoch genausogut auch auf die Seiteninformationen, wie z. B. Skalenfaktoren, in Abhängigkeit des Benutzerschlüssels k eingreifen. Werden, wie bei dem in Fig. 3 gezeigten Ausführungsbeispiel, Entropie-codierte quantisierte Spektralwerte lediglich umsortiert, so tritt keine Veränderung der Länge des verschlüsselten Datenstroms am Ausgang 14 der Verschlüsselungsvorrichtung 10 auf, derart, daß der codierte verschlüsselte Datenstrom in denselben Übertragungskanal wie

der unverschlüsselte decodierte Datenstrom paßt.

In Fig. 4 ist ein weiteres bevorzugtes Ausführungsbeispiel gezeigt, bei dem die Verwürfelungseinheit 180 zwischen den Entropie-Codierer 210 und den Quantisierer 206 geschaltet ist. Hier werden quantisierte Spektralwerte, die noch nicht Entropie-codiert worden sind, im einfachsten Fall verwürfelt. Dies bedeutet, daß im Gegensatz zu Fig. 3 nun die verwürfelten quantisierten Spektralwerte Entropie-codiert werden.

Lediglich beispielhaft wird im nachfolgenden eine an sich bekannte Scrambling- bzw. Verwürfelungsfunktion beschrieben, die als sogenannter Keimerzeugungsalgorithmus ("Seed-Generating"-Algorithmus) ausgeführt ist. Hierbei wird ein Zufallszahlengenerator verwendet, der abhängig von einem bestimmten Startwert, d. h. dem Keim, eine Zufallszahlenfolge ermittelt. Wesentlich daran ist, daß der Zufallszahlengenerator immer wieder die gleiche Zufallszahlenfolge liefern wird, wenn er denselben Startwert erhält, daß er jedoch eine andere Zufallszahlenfolge ergeben wird, wenn er einen anderen Startwert erhält. Der Startwert würde in diesem Beispiel der Schlüssel k sein. Die quantisierten Spektralwerte (in Fig. 4) können nun mit der Pseudo-Zufallsbitfolge bitweise mittels z. B. einer XOR-Funktion verknüpft werden. Damit werden bestimmte Bits der quantisierten Spektralwerte verändert, was eine Verschlüsselung darstellt, die nur durch eine Vorrichtung zum Erzeugen eines entschlüsselten Datenstroms wieder rückgängig gemacht werden kann, die denselben Schlüssel, d. h. denselben Startwert, für ihren Zufallszahlengenerator aufweist, der wieder eine XOR-Verknüpfung der quantisierten Spektralwerte mit den verwürfelten quantisierten Spektralwerten durchführt, wie später detaillierter ausgeführt wird. Es sei darauf hingewiesen, daß die XOR-Verknüpfung nur ein Beispiel für eine eindeutig umkehrbare Veränderung ist. Die XOR-Funktion hat den Vorteil, daß eine doppelte Anwendung der gleichen Funktion wieder zum Ausgangspunkt führt, derart, daß nur eine einzige Funktion und nicht eine erste

Funktion und eine zweite Umkehrfunktion implementiert werden müssen. Prinzipiell ist aber jede umkehrbare Funktion zur Verknüpfng geeignet.

Wenn durch die Verschlüsselungseinrichtung nicht sämtliche Bits eines quantisierten Spektralwerts beeinflußt werden, sondern lediglich die niederwertigen Bits, so wird die Verschlüsselung "weicher" sein, derart, daß der verschlüsselte Audiostrom nur auf begrenzte Art und Weise beeinflußt worden ist und noch eine relativ gute hörbare Qualität haben wird. Somit ist ersichtlich, daß gemäß der vorliegenden Erfindung die Intensität der Verschlüsselung nahezu beliebig eingestellt werden kann. Wird eine sehr massive Verschlüsselung erwünscht, so ist es möglich, die Skalenfaktoren direkt zu beeinflussen. Bei bestimmten Codierverfahren tragen dieselben jedoch die wesentlichen Intensitätsinformationen, weshalb eine Beeinflussung der Skalenfaktoren zu ganz erheblichen Beeinträchtigungen der Audioqualität führen kann.

Im vorhergehenden wurde bereits eine einfache Funktionsweise der Verschlüsselungseinrichtung 18 mit der Verwürfelungseinrichtung 180 beschrieben. Wird eine Beeinflussung der quantisierten Spektralwerte bereits vor der Entropie-Codierung durchgeführt, so wird dies sehr wahrscheinlich zu einer veränderten Länge des Bitstroms am Ausgang 14 der Vorrichtung 10 führen, da die bitweise veränderten quantisierten Spektralwerte sehr wahrscheinlich andere Codewörter mit unterschiedlicher Länge nach sich ziehen werden als die unverwürfelten Spektralwerte, die von dem Codierer 16 erzeugt werden würden, wenn keine Verschlüsselungseinrichtung 18 vorhanden sein würde. Werden dagegen, wie es in Fig. 3 gezeigt ist, die Codewörter nach der Entropie-Codierung 210 nur umsortiert, so wird dies nicht zu einer größeren Länge des Bitstroms am Ausgang 14 führen.

Es existieren jedoch noch viele weiteren Möglichkeiten, um codiererinterne Daten zu beeinflussen. Bei Audiocodierern gemäß dem eingangs beschriebenen AAC-Standard wird eine En-

tropie-Codierung durchgeführt, die dort als "Noiseless Coding" bezeichnet wird. Dieselbe wird verwendet, um die Redundanz der Skalenfaktoren und des quantisierten Spektrums jedes Audiokanals weiter zu reduzieren. Als Entropie-Codierverfahren wird ein Huffman-Codierverfahren eingesetzt. Insbesondere werden für bestimmte Abschnitte oder Sections, die aus mehreren Skalenfaktorbändern bestehen können, jeweilige Codetabellen (Codebooks) verwendet. Insbesondere existieren 11 verschiedene normierte Codetabellen, die durch eine Codetabellennummer jeweils eindeutig identifiziert werden. Der Entropiecodierer 210 ordnet somit jedem Abschnitt, der mit ein und derselben Codetabelle Entropie-codiert wird, die entsprechende Codetabellennummer zu. Die Verwürfelungseinrichtung 180 könnte nun bereits die Codetabellennummer verändern. Diese Veränderung ist jedoch lediglich in begrenztem Rahmen möglich, um eine umkehrbare Veränderung im Rahmen der Bitstromsyntax zu erreichen. So existieren Codetabellen, die vorzeichenbehaftete oder vorzeichenlose n-Tupel von quantisierten Spektralwerten darstellen können. Außerdem existieren Codetabellen, die vierdimensional sind, oder die zweidimensional sind. Dies bedeutet, daß ein Codewort vier quantisierte Spektralwerte im Falle einer vierdimensionalen Codetabelle, oder zwei quantisierte Spektralwerte im Falle einer zweidimensionalen Codetabelle darstellt.

Manche Codetabellen stellen eine vorzeichenbehaftete Entropie-Codierung von Spektralwerten dar, während wieder andere Codetabellen eine vorzeichenlose Codierung von Spektralwerten darstellen. Wenn die Codetabellen vorzeichenlos codieren, wird dem Codewort unmittelbar ein Vorzeichenbit für jeden Spektralwert im Bitstrom hinterhergestellt, wenn der entsprechende Spektralswert ungleich Null ist. Ein Decodierer kann dann aufgrund des Huffman-Codeworts und des folgenden Vorzeichenbits den quantisierten Spektralwert wieder decodieren. Die Verschlüsselungseinrichtung 18 ist bei einem bevorzugten Ausführungsbeispiel der vorliegenden Erfindung angepaßt, um eine Vorzeichenänderung der quantisierten Spektralwerte, die mit vorzeichenlosen Codetabellen codiert

werden, durchzuführen. Die Vorzeichenänderung geschieht durch Verändern des beschrieben Vorzeichens, wobei diese Veränderung entweder nach einem bestimmten Muster oder unter Verwendung einer XOR-Verknüpfung einer Pseudo-Zufallsbitfolge mit den Vorzeichendaten durchgeführt werden könnte. Damit wird immer die gleiche Länge des resultierenden Bitstroms erreicht, wenn nur die quantisierten Spektralwerte beeinflußt werden, die mit vorzeichenlosen Codetabellen Entropie-codiert werden.

Wie es bereits erwähnt wurde, wird beim AAC-Standard ein Abschnitt ("Section"), d. h. ein bestimmtes Frequenzband des Kurzzeitspektrums des Audiosignals, das zumindest ein Skalenfaktorband aufweist, mit ein und derselben Codetabelle Entropie-codiert. Wenn die Verwürfelungseinrichtung 180 derart gestaltet ist, daß sie lediglich eine Umsortierung der quantisierten Spektralwerte in ihrem Frequenzraster ohne eine Veränderung der quantisierten Spektralwerte selbst durchführt, so kann eine gleiche Länge des ausgangsseitigen Bitstroms am Ausgang 14 der Vorrichtung 10 zum Erzeugen eines verschlüsselten Datenstroms erreicht werden, wenn nur innerhalb von Spektralbereichen umsortiert wird, in denen die Codierung der quantisierten Spektralwerte mit der gleichen Art der Entropiecodierung, z. B. dem gleichen Huffman-Codebook, vorgenommen wird.

Eine gleiche Länge des verschlüsselten codieren Datenstroms wird ferner erreicht, wenn im Falle der Verwendung von mehrdimensionalen Codetabellen statt einzelnen quantisierten Spektralwerten n-Tupel von Spektralwerten gemeinsam umsortiert werden.

Damit wird ein codierter verschlüsselter Datenstrom am Ausgang 14 der Vorrichtung 10 zum Erzeugen eines verschlüsselten Datenstroms erzeugt, der die gleiche Datenstromsyntax hat, wie sie für bzw. durch den Codierer 16 vorbestimmt ist, und der darüberhinaus bei besonders bevorzugten Ausführungsbeispielen der vorliegenden Erfindung die gleiche Länge wie

ein unverschlüsselter codierter Datenstrom aufweist.

In den Fig. 5 und 6 sind entsprechende Vorrichtungen 30 zum Erzeugen eines entschlüsselten Audio- und/oder Videosignals dargestellt. So ist die Vorrichtung 30, die in Fig. 5 skizziert ist, komplementär zu der Vorrichtung zum Erzeugen eines entschlüsselten Datenstroms in Fig. 3. Analog ist die in Fig. 6 dargestellte Vorrichtung 30 zum Erzeugen eines entschlüsselten Audio- und/oder Videosignals zu der in Fig. 4 dargestellten Vorrichtung 10 zum Erzeugen eines verschlüsselten Datenstroms komplementär. Die Entschlüsselungseinrichtung 38 in den Fig. 5 und 6 enthält eine Einheit 380 zum Durchführen einer inversen Verwürfelung (Descrambling), um die durch die Verwürfelungseinrichtung 180 (Fig. 3, Fig. 4) eingeführten Beeinflussungen der codiererinternen Daten, d. h. der Entropie-codierten quantisierten Spektralwerte bzw. der quantisierten Spektralwerte, die noch nicht Entropie-codiert worden sind, wieder rückgängig zu machen.

Grundsätzlich kann gesagt werden, daß die Funktion der Einrichtung 380 zur inversen Verwürfelung immer komplementär zu der dazugehörigen Einrichtung 180 zum Verwürfeln ist. Eine Verwendung eines Keimerzeugungsalgorithmus, d. h. einer Schlüssel-gesteuerten Pseudo-Zufallsbitfolge, erlaubt es, daß die Einrichtung 180 und die entsprechende Einrichtung 380 exakt gleich aufgebaut werden können und der Schlüssel zum Verschlüsseln dem Schlüssel zum Entschlüsseln exakt entspricht. Andere Lösungen, bei denen die Verschlüsselungseinrichtung 180 und die Entschlüsselungseinrichtung 380 unterschiedlich aufgebaut sind, und bei denen die Schlüssel zum Verschlüsseln und zum Entschlüsseln nicht identisch sind, sondern in einem bestimmten Zusammenhang zueinander stehen, können jedoch ebenfalls eingesetzt werden, solange die Verschlüsselungseinrichtung eindeutig umkehrbare Veränderungen an den entsprechenden Daten auf der Basis des Schlüssels durchführt und die Vorrichtung zum Erzeugen eines entschlüsselten Audio- und/oder Videosignals die eingeführten Änderungen auf der Basis des Schlüssels wieder rückgängig machen

kann.

Während bezüglich der Fig. 3 und 4 bevorzugte Ausführungsbeispiele der vorliegenden Erfindung zum Erzeugen eines verschlüsselten Datenstroms am Ausgang 14 beschrieben worden sind, die aus einem zeitdiskreten Audiosignal am Eingang 12 den verschlüsselten Datenstrom am Ausgang 14 erzeugen, wird nun anhand von Fig. 7 eine erfindungsgemäße Vorrichtung zum Erzeugen eines verschlüsselten Datenstroms gemäß einem weiteren Ausführungsbeispiel der vorliegenden Erfindung beschrieben, die den verschlüsselten Datenstrom an ihrem Ausgang erzeugt, jedoch nicht aus einem zeitdiskreten Eingangssignal sondern aus einem andersartig verschlüsselten (codierten) Datenstrom.

Die in Fig. 7 gezeigte Vorrichtung 70 zum Erzeugen des verschlüsselten Datenstroms erzeugt an ihrem Ausgang 72 einen mit einem Schlüssel k_2 verschlüsselten, codierten Datenstrom, während sie an ihrem Eingang 74 einen mit einem zu k_2 unterschiedlichen Schlüssel k_1 verschlüsselten, codierten Datenstrom empfängt. Die Vorrichtung 70 erzeugt nun nicht mehr aus einem zeitdiskreten Audio-Eingangssignal einen verschlüsselten Datenstrom, sondern allgemein aus einem mit einem ersten Schlüssel verschlüsselten Datenstrom einen mit einem anderen Schlüssel verschlüsselten Datenstrom. Die Vorrichtung 70 umfaßt abweichend von Fig. 1 eine Verschlüsselungseinrichtung 18 und einen Teil-Codierer 16'. Die Vorrichtung 70 umfaßt ferner eine Entschlüsselungseinrichtung 38 und einen Teil-Decodierer 36'. Im Gegensatz zu den in den Fig. 3 und 4 beschriebenen Ausführungsbeispielen besteht der Teil-Decodierer 36' nur noch aus einem Bitstrom-Demultiplexer 222 und einem Entropie-Decodierer 224, während der Teil-Codierer 16' nun lediglich noch aus einem Entropie-Codierer 210 und einem Bitstrom-Multiplexer 212 besteht. Die in Fig. 7 gezeigte Verschlüsselungseinrichtung 18 beeinflußte die Eingangsdaten des Teil-Codierers 16', während analog dazu die Entschlüsselungseinrichtung 38 von Fig. 7 die Ausgangsdaten des Teil-Decodierers 36 beeinflußt. Die

Ausgangsdaten aus dem Teil-Decodierer sind in der bisherigen Terminologie die decodiererinternen Daten, d. h. die Daten, die bei der Erzeugung des in die Einrichtung 70 eingespeisten verschlüsselten Datenstroms ursprünglich beeinflußt worden sind. Die Eingangsdaten in den Teil-Codierer der Vorrichtung 70 sind analog dazu die codiererinternen Daten des Codieres, der den verschlüsselten, codierten Datenstrom am Eingang ursprünglich erzeugt hat.

Im nachfolgenden wird auf die Funktionsweise der Vorrichtung 70 zum Erzeugen eines verschlüsselten Datenstroms, wie sie in Fig. 7 gezeigt ist, eingegangen. Am Eingang 74 erhält die Vorrichtung 70 einen mit einem Schlüssel k_1 verschlüsselten codierten Datenstrom, der bei der hier gezeigten Ausführungsform derart verschlüsselt worden ist, daß die quantisierten Spektralwerte vor ihrer Entropie-Codierung verwürfelt worden sind, oder, allgemeiner gesagt, auf irgendeine Art und Weise auf der Basis des Schlüssels k_1 auf umkehrbare Art und Weise beeinflußt worden sind. Am Ausgang des Entropie-Decodierers 224 liegen dann die noch verschlüsselten jedoch Entropie-decodierten quantisierten Spektralwerte vor, die durch die Entschlüsselungseinrichtung 38 auf der Basis des Schlüssel k_1 unter Verwendung der Einrichtung 380 zum Durchführen einer inversen Verwürfelung wieder entschlüsselt werden, derart, daß zwischen dem Teil 30' und dem Teil 10' ein decodierter Datenstrom vorliegt, der nun jedoch nicht ein zeitdiskretes Audio- und/oder Videosignal oder etwas ähnliches ist, sondern der bei dem in Fig. 7 gezeigten Ausführungsbeispiel quantisierte Spektralwerte, d. h. codiererinterne bzw. decodiererinterne Daten umfaßt. Die quantisierten Spektralwerte werden in die Verschlüsselungseinrichtung 18 und insbesondere in die Verwürfelungseinrichtung 180 eingespeist, derart, daß dieselben auf der Basis eines von dem Schlüssel k_1 unterschiedlichen Schlüssels k_2 verwürfelt oder allgemeiner gesagt beeinflußt werden, um dann in dem Teil-Codierer 16' Entropie-codiert zu werden, damit sich an dem Ausgang 72 schließlich ein mit dem Schlüssel k_2 verschlüsselter codierter Datenstrom ergibt. Aus Fig. 7 ist er-

sichtlich, daß es sich hier um einen sogenannten "Scrambling-Transcoder" handelt, d. h. um einen Bitstromkonvertierer, welcher einen mit einem Schlüssel k_1 verschlüsselten Bitstrom direkt in einen Bitstrom mit dem Schlüssel k_2 umsetzt. Derselbe umfaßt nicht mehr einen vollständigen Audio-Decodierer oder Audio-Codierer, sondern lediglich noch bestimmte Teile derselben, die im Sinne dieser Erfindung als Teil-Decodierer bzw. Teil-Codierer bezeichnet werden.

Fig. 8 zeigt eine allgemeine Darstellung einer Vorrichtung 70' zum Erzeugen eines verschlüsselten codierten Datenstroms, die sich nur darin von der in Fig. 7 gezeigten Vorrichtung unterscheidet, daß der Bitstrom am Eingang 74' ein codierter nicht-verschlüsselter Datenstrom ist, der durch den Teil-Decodierer 36' decodiert wird und dann durch den Teil-Codierer 16' in Verbindung mit der Verschlüsselungseinrichtung 18 codiert und verschlüsselt wird, derart, daß sich an dem Ausgang 72' ein verschlüsselter/codierter Datenstrom ergibt. Die in Fig. 8 gezeigte Vorrichtung 70' könnte beispielsweise dazu verwendet werden, einen Standard-Bitstrom mit der vordefinierten Datenstromsyntax direkt in einen mit einem bestimmten Schlüssel verschlüsselten Datenstrom umzusetzen, wobei beide Datenströme die vordefinierte Datenstromsyntax aufweisen.

Fig. 9 zeigt ein weiteres Ausführungsbeispiel einer erfindungsgemäßen Vorrichtung 80 zum Erzeugen eines entschlüsselten Datenstroms mit einem Ausgang 82 und einem Eingang 84. Am Eingang 84 wird ein codierter/verschlüsselter Datenstrom eingespeist, der unter Verwendung der Einrichtung 38, die mit dem Teil-Decodierer 36 gekoppelt ist, entschlüsselt wird, derart, daß sich ein decodierter entschlüsselter Datenstrom ergibt, der wiederum in einen nachgeschalteten Teil-Codierer 16 eingespeist wird, derart, daß sich ein codierter/nicht-verschlüsselter Datenstrom ergibt. Die in Fig. 9 dargestellte Vorrichtung 80 zum Erzeugen eines verschlüsselten Datenstroms ist somit ein Bit- bzw. Datenstromkonvertierer, welcher einer mit einem Schlüssel k_1 ver-

schlüsselten Bitstrom direkt in einen Standard-Bitstrom, d. h. in einen Bitstrom, der nicht-verschlüsselt ist und die vordefinierte Datenstromsyntax aufweist, umsetzt.

Abweichend von den beschriebenen Ausführungsbeispielen für die Vorrichtungen 70, 70' und 80 können sämtliche in dieser Anmeldung beschriebenen Beeinflussungen von codiererinternen Daten auf sämtliche beschriebenen Arten und Weisen durchgeführt werden. Im Hinblick auf das vorhergehende ist es offensichtlich, daß die Teil-Codierer bzw. Teil-Decodierer an die entsprechende Beeinflussung angepaßt werden können. Wurde z. B. eine Umsortierung von Huffman-Codewörtern durchgeführt, so könnte ein Teil-Decodierer lediglich einen Bitstrom-Demultiplexer enthalten, während der Teil-Codierer dann lediglich einen Bitstrom-Multiplexer umfaßt.

Patentansprüche

1. Vorrichtung (10) zum Erzeugen eines verschlüsselten Datenstroms aus einem Audio- und/oder Videosignal, mit folgenden Merkmalen:

einem Codierer (16) zum Codieren des Audio- und/oder Videosignals, um als Ausgangssignal einen Datenstrom mit einer vordefinierten Datenstromsyntax zu erzeugen;

einer Verschlüsselungseinrichtung (18), die mit dem Codierer (16) gekoppelt ist, zum Beeinflussen von codiererinternen Daten (20a) und/oder des Ausgangssignals (20b) des Codierers (16) auf eine eindeutig umkehrbare Art und Weise auf der Basis eines Schlüssels (k_1), derart, daß der erzeugte verschlüsselte Datenstrom Nutzinformationen aufweist, die sich von Nutzinformationen eines Datenstroms unterscheiden, der durch die Vorrichtung (10) ohne Vorhandensein der Verschlüsselungseinrichtung (18) erzeugt werden würde, und daß der erzeugte verschlüsselte Datenstrom die vordefinierte Datenstromsyntax aufweist.

2. Vorrichtung nach Anspruch 1, bei der die Verschlüsselungseinrichtung (18) ferner angeordnet ist, um auf der Basis des Schlüssels die codiererinternen Daten (20a) und/oder die Ausgangsdaten (20b) des Codierers (16) so zu beeinflussen, daß der verschlüsselte Datenstrom die gleiche Länge in Bit hat wie ein Datenstrom, der durch die Vorrichtung (10) ohne Vorhandensein der Verschlüsselungseinrichtung erzeugt werden würde.

3. Vorrichtung nach einem der vorhergehenden Ansprüche, bei der die Verschlüsselungseinrichtung (18) angeordnet ist, um auf der Basis des Schlüssels die codiererinternen Daten (20a) und/oder die Ausgangsdaten (20b) des Codierers lediglich so stark zu beeinflussen, daß sich die Nutzinformationen des verschlüsselten Datenstroms

nur so stark von den Nutzinformationen eines Datenstroms unterscheiden, der ohne Vorhandensein der Verschlüsselungseinrichtung (18) erzeugt werden würde, daß ein Decodierer, der nicht im Besitz des Schlüssels ist, aufgrund der verschlüsselten Daten ein decodiertes Ausgangssignal mit einer Qualität liefert, die geringer als die Qualität ist, die der Decodierer liefern würde, wenn er im Besitz des Schlüssels wäre, wobei jedoch eine Mindestqualität sichergestellt ist.

4. Vorrichtung nach einem der vorhergehenden Ansprüche, bei der die Verschlüsselungseinrichtung (18) angeordnet ist, um lediglich die codiererinternen Daten (20a) zu beeinflussen.

5. Vorrichtung nach einem der Ansprüche 1 bis 4, bei der der Codierer ein Codierer für Audiosignale ist, der folgende Merkmale aufweist:

eine Analysefilterbank (204) zum Umsetzen des Audiosignals von dem Zeitbereich in eine spektrale Darstellung, um Spektralwerte zu erhalten; und

eine Quantisierungseinrichtung (206) zum Quantisieren der Spektralwerte unter Berücksichtigung eines psychoakustischen Modells (208), die quantisierte Spektralwerte als Hauptinformationen und Skalenfaktoren, von denen jeder mindestens einem quantisierten Spektralwert zugeordnet ist, als Seiteninformationen erzeugt; und

bei der die Verschlüsselungseinrichtung (18) angeordnet ist, um die durch die Quantisierungseinrichtung (206) erzeugten Skalenfaktoren auf der Basis des Schlüssels zu beeinflussen.

6. Vorrichtung nach einem der Ansprüche 1 bis 4, bei der der Codierer ein Codierer für Audiosignale ist, der folgende Merkmale aufweist:

eine Analysefilterbank (204) zum Umsetzen des Audiosignals in eine spektrale Darstellung, um Spektralwerte zu erhalten; und

eine Quantisierungseinrichtung (206) zum Quantisieren der Spektralwerte unter Berücksichtigung eines psychoakustischen Modells (208), die quantisierte Spektralwerte als Hauptinformationen und Skalenfaktoren, von denen jeder mindestens einem quantisierten Spektralwert zugeordnet ist, als Seiteninformationen erzeugt; und

bei der die Verschlüsselungseinrichtung (18) angeordnet ist, um die quantisierten Spektralwerte, die durch die Einrichtung (206) zum Quantisieren erzeugt werden, zu beeinflussen.

7. Vorrichtung nach Anspruch 6, bei der die Verschlüsselungseinrichtung (18) angeordnet ist, um die quantisierten Spektralwerte auf der Basis des Schlüssels umzusortieren.

8. Vorrichtung nach Anspruch 6 oder 7, bei der die Verschlüsselungseinrichtung angeordnet ist, um zumindest einen Teil der quantisierten Spektralwerte mit einer Pseudo-Zufallsbitfolge, die aufgrund des Schlüssels als Startwert erzeugt wird, mittels einer EXKLUSIV-ODER-Verknüpfung zu verknüpfen.

9. Vorrichtung nach einem der Ansprüche 6 bis 8, bei der lediglich niederwertige Bits von Spektralwerten mit einer Pseudo-Zufallsbitfolge verknüpft werden.

10. Vorrichtung nach einem der Ansprüche 6 bis 9, bei der die quantisierten Spektralwerte vorzeichenbehaftet sind, und bei der die Verschlüsselungseinrichtung (18) angeordnet ist, um auf der Basis des Schlüssels Vorzeichen von quantisierten Spektralwerten zu verändern.

11. Vorrichtung nach einem der Ansprüche 6 bis 10,

bei der der Codierer (16) ferner einen Entropie-Codierer (210) aufweist, der angeordnet ist, um eine Entropie-Codierung der quantisierten Spektralwerte mittels einer Mehrzahl von vordefinierten Codetabellen durchzuführen.

12. Vorrichtung nach Anspruch 11, bei der der Entropie-Codierer (210) derart angeordnet ist, daß er zumindest eine Codetabelle aufweist, die eine vorzeichenlose Codetabelle ist, derart, daß ein Vorzeichen für ein Codewort aus der Codetabelle getrennt von dem Codewort in die Nutzinformationen geschrieben wird, wobei die Verschlüsselungseinrichtung (18) angeordnet ist, um vor der Entropie-Codierung der quantisierten Spektralwerte das Vorzeichen zumindest eines quantisierten Spektralwerts basierend auf dem Schlüssel zu verändern.

13. Vorrichtung nach Anspruch 11 oder 12, bei der jede Codetabelle für die Entropiecodierung von quantisierten Spektralwerten in einem bestimmten Frequenzband mit zumindest einem Spektralwert vorgesehen ist, wobei zumindest ein Frequenzband zwei oder mehrere quantisierte Spektralwerte aufweist, und wobei die Verschlüsselungseinrichtung (18) angeordnet ist, um basierend auf dem Schlüssel die zwei oder mehr quantisierten Spektralwerte in dem Frequenzband, das zwei oder mehr quantisierte Spektralwerte aufweist, umzusortieren.

14. Vorrichtung nach einem der Ansprüche 11 bis 13, bei der zumindest eine Codetabelle der Mehrzahl von Codetabellen eine mehrdimensionale Codetabelle ist, bei der ein Codewort eine Mehrzahl von quantisierten Spektralwerten darstellt, wobei die Verschlüsselungseinrichtung (18) angeordnet ist, um Gruppen von quantisierten Spektralwerten umzusortieren, wobei eine Gruppe von Spektral-

werten so viele quantisierte Spektralwerte aufweist, wie sie durch ein Codewort der mehrdimensionalen Codetabelle codiert werden.

15. Vorrichtung nach einem der Ansprüche 1 bis 3, bei der die Ausgangsdaten des Codierers (16) eine Folge von Codewörtern enthält, wobei die Folge von Codewörtern eine entropiecodierte Version des Audio- und/oder Videosignals darstellt, wobei die Verschlüsselungseinrichtung (18) zum Beeinflussen der Ausgangsdaten (20b) des Codierers angeordnet ist, um die Folge der Codewörter basierend auf dem Schlüssel umzusortieren.

16. Vorrichtung nach einem der vorhergehenden Ansprüche, bei der der Codierer eine Mehrzahl von Unterblöcken (204 bis 210) aufweist, die mit einem Bitstrommultiplexer (212) verbunden sind, der von den einzelnen Unterblöcken ausgegebene Daten gemäß der vordefinierten Datenstromsyntax multiplext, um die Ausgangsdaten des Codierers (16) zu erhalten.

17. Vorrichtung (70) zum Erzeugen eines auf der Basis eines zweiten Schlüssels (k_2) verschlüsselten Datenstroms aus einem auf der Basis eines ersten Schlüssels (k_1) verschlüsselten ersten Datenstroms, wobei der erste Datenstrom ein unter Verwendung eines Codierers codiertes Audio- und/oder Videosignal mit einer vordefinierten Datenstromsyntax ist, wobei der erste Datenstrom derart verschlüsselt ist, daß codiererinterne Daten auf der Basis des ersten Schlüssels (k_1) beeinflußt worden sind, mit folgenden Merkmalen:

einem Teil-Decodierer (36') zum Rückgängigmachen eines Teils der Codierung, derart, daß die beeinflußten codiererinternen Daten vorliegen;

einer Entschlüsselungseinrichtung (38) zum Entschlüsseln der codiererinternen Daten auf der Basis des er-

sten Schlüssels (k_1);

einer Verschlüsselungseinrichtung (18) zum Beeinflussen der codiererinternen Daten auf der Basis des zweiten Schlüssels (k_2);

einem Teil-Codierer (16') zum Durchführen des Teils der Codierung, der durch den Teil-Decodierer (36') rückgängig gemacht worden ist, um den auf der Basis des zweiten Schlüssels (k_2) verschlüsselten Datenstrom zu erzeugen, wobei der zweite Datenstrom die vordefinierte Datenstromsyntax aufweist.

18. Vorrichtung (70') zum Erzeugen eines auf der Basis eines Schlüssels (k_1) verschlüsselten zweiten Datenstroms aus einem ersten Datenstrom, wobei der erste Datenstrom ein unter Verwendung eines Codierers codiertes Audio- und/oder Videosignal mit einer vordefinierten Datenstromsyntax ist, mit folgenden Merkmalen:

einem Teil-Decodierer (36') zum Rückgängigmachen eines Teils der Codierung, derart, daß zu beeinflussende codiererinterne Daten vorliegen;

einer Verschlüsselungseinrichtung (18) zum Beeinflussen der codiererinternen Daten auf der Basis des Schlüssels (k_1);

einem Teil-Codierer (16') zum Durchführen des Teils der Codierung, der durch den Teil-Decodierer (36') rückgängig gemacht worden ist, um den auf der Basis des Schlüssels (k_1) verschlüsselten Datenstrom zu erzeugen, wobei der zweite Datenstrom die vordefinierte Datenstromsyntax aufweist.

19. Vorrichtung (80) zum Erzeugen eines entschlüsselten Datenstroms aus einem auf der Basis eines Schlüssels (k_1) verschlüsselten ersten Datenstroms, wobei der erste Da-

tenstrom ein unter Verwendung eines Codierers codiertes Audio- und/oder Videosignal mit einer vordefinierten Datenstromsyntax ist, wobei der erste Datenstrom derart verschlüsselt ist, daß codiererinterne Daten auf der Basis des ersten Schlüssels (k_1) beeinflußt worden sind, mit folgenden Merkmalen:

einem Teil-Decodierer (36') zum Rückgängigmachen eines Teils der Codierung, derart, daß die beeinflußten codiererinternen Daten vorliegen;

einer Entschlüsselungseinrichtung (38) zum Entschlüsseln der codiererinternen Daten auf der Basis des Schlüssels (k_1);

einem Teil-Codierer (16') zum Durchführen des Teils der Codierung, der durch den Teil-Decodierer (36') rückgängig gemacht worden ist, um den zweiten Datenstrom mit der vordefinierten Datenstromsyntax zu erzeugen.

20. Vorrichtung nach einem der Ansprüche 17 bis 19,

bei der der Teil-Decodierer (36') einen Bitstrom-Demultiplexer (222) aufweist, wobei die codiererinternen Daten die Ausgangsdaten aus dem Bitstrom-Demultiplexer (222) sind.

21. Vorrichtung nach Anspruch 20,

bei der der Teil-Decodierer (36') fernen einen dem Bitstrom-Demultiplexer (222) nachgeschalteten Entropie-Decodierer (224) aufweist, wobei die codiererinternen Daten die Ausgangsdaten aus dem Entropie-Decodierer (224) sind.

22. Vorrichtung nach einem der Ansprüche 17 bis 19, bei der die codiererinternen Daten quantisierte Spektralwerte und/oder Skalenfaktoren sind.

23. Vorrichtung (30) zum Erzeugen eines entschlüsselten Audio- und/oder Videosignals aus einem verschlüsselten Datenstrom, der ein Audio- und/oder Videosignal darstellt, wobei der verschlüsselte Datenstrom Nutzinformationen aufweist, die sich von Nutzinformationen eines unverschlüsselten Datenstroms unterscheiden, und wobei der verschlüsselte Datenstrom dieselbe Datenstromsyntax wie ein unverschlüsselter Datenstrom aufweist, mit folgenden Merkmalen:

einem Decodierer (36) zum Decodieren von Eingangsdaten, um decodierte Ausgangsdaten zu erzeugen; und

einer Entschlüsselungseinrichtung (38) zum Beeinflussen des verschlüsselten Datenstroms (40a) und/oder von decodiererinternen Daten (40b) auf der Basis eines Schlüssels, um die eindeutig umkehrbaren Veränderungen, die in einer Vorrichtung zum Erzeugen eines verschlüsselten Datenstroms durchgeführt worden sind, rückgängig zu machen, um das entschlüsselte Audio- und/oder Videosignal zu erhalten.

24. Vorrichtung nach Anspruch 23,

bei der der verschlüsselte Datenstrom quantisierte Spektralwerte aufweist, die durch eine Verschlüsselungseinrichtung beeinflußt worden sind; und

bei der die Entschlüsselungseinrichtung (38) angeordnet ist, um die Beeinflussung der quantisierten Spektralwerte rückgängig zu machen.

25. Vorrichtung nach Anspruch 24, bei der der Decodierer (36) folgende Merkmale aufweist:

einen Entropie-Decodierer (24) zum Rückgängigmachen der Entropie-Codierung, um die beeinflußten quantisierten

Spektralwerte zu erhalten.

26. Vorrichtung nach Anspruch 24, bei der der Decodierer (36) ferner folgendes Merkmal aufweist:

einen Entropie-Decodierer (224) zum Rückgängigmachen der Entropie-Codierung, in den die unbeeinflußten quantisierten Spektralwerte einspeisbar sind; und

bei der die Entschlüsselungseinrichtung (38) angeordnet ist, um die Beeinflussung der Entropie-codierten Spektralwerte rückgängig zu machen.

27. Vorrichtung (30) nach einem der Ansprüche 23 bis 26, bei der der Decodierer ferner folgende Merkmale aufweist:

eine Mehrzahl von Funktionsblöcken, die mit einem Bitstrom-Demultiplexer (222) gekoppelt sind, der Teile des Datenstroms gemäß der vordefinierten Datenstromsyntax zu den einzelnen Blöcken leitet.

28. Vorrichtung (30) nach einem der Ansprüche 23 bis 27, bei der der Decodierer (36) ferner folgendes Merkmal aufweist:

eine Synthesefilterbank (228), um eine spektrale Darstellung des Audio- und/oder Videosignals in eine zeitliche bzw. örtliche Darstellung umzusetzen.

29. Verfahren zum Erzeugen eines verschlüsselten Datenstroms, der ein Audio- und/oder Videosignal darstellt, mit folgenden Schritten:

Codieren (16) eines Eingangssignals, um als Ausgangssignal einen codierten Datenstrom mit einer vordefinierten Datenstromsyntax zu erzeugen;

wobei während des Schritts des Codierens und/oder nach dem Schritt des Codierens folgender Schritt ausgeführt wird:

Beeinflussen von Daten während des Codierens (20a) und/oder des Ausgangssignals (20b) auf eine eindeutig umkehrbare Art und Weise auf der Basis eines Schlüssels, derart, daß der erzeugte verschlüsselte Datenstrom Nutzinformationen aufweist, die sich von Nutzinformationen eines Datenstroms unterscheiden, der durch den Schritt des Codierens ohne den Schritt des Beeinflussens erzeugt werden würde, und daß der erzeugte verschlüsselte Datenstrom die vordefinierte Datenstromsyntax aufweist.

30. Verfahren zum Erzeugen eines entschlüsselten Datenstroms aus einem verschlüsselten Datenstrom, der ein Audio- und/oder Videosignal darstellt, wobei der verschlüsselte Datenstrom Nutzinformationen aufweist, die sich von Nutzinformationen eines unverschlüsselten Datenstroms unterscheiden, und wobei der verschlüsselte Datenstrom dieselbe Datenstromsyntax wie ein unverschlüsselter Datenstrom aufweist, mit folgenden Schritten:

Decodieren (36) von Eingangsdaten, um decodierte Ausgangsdaten zu erhalten; und

wobei vor dem Schritt des Decodierens und/oder während des Schritts des Decodierens folgender Schritt ausgeführt wird:

Beeinflussen (38) der Eingangsdaten (40a) und/oder von Daten (40b) während des Decodierens auf der Basis eines Schlüssels, der zum Verschlüsseln verwendet wurde, derart, daß der verschlüsselte Datenstrom entschlüsselt wird.

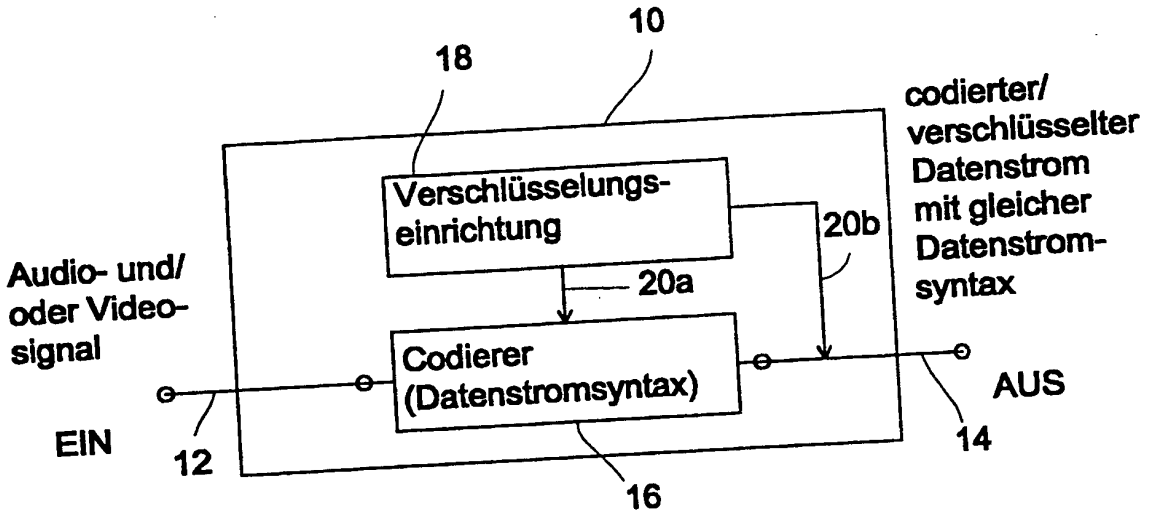

10
18
codierter/
verschlüsselter
Datenstrom
mit gleicher
Datenstrom-
syntax
Verschlüsselungs-
einrichtung
20b
20a
Audio- und/
oder Video-
signal
Codierer
(Datenstromsyntax)
AUS
EIN
12
14
16

Fig. 1

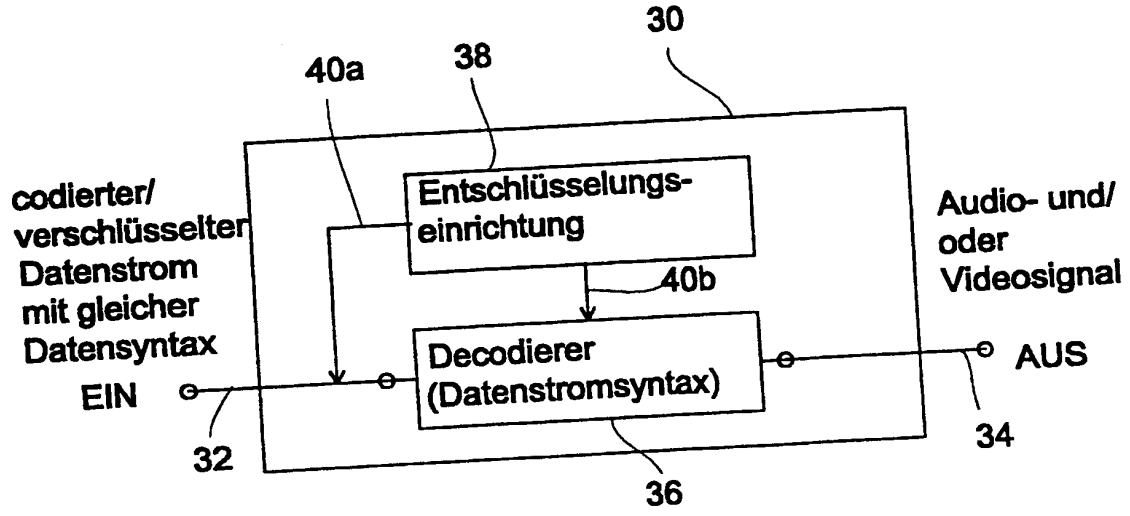

30
40a
38
codierter/
verschlüsselter
Datenstrom
mit gleicher
Datensyntax
Entschlüsselungs-
einrichtung
Audio- und/
oder
Videosignal
40b
Decodierer
(Datenstromsyntax)
AUS
EIN
32
34
36

Fig. 2

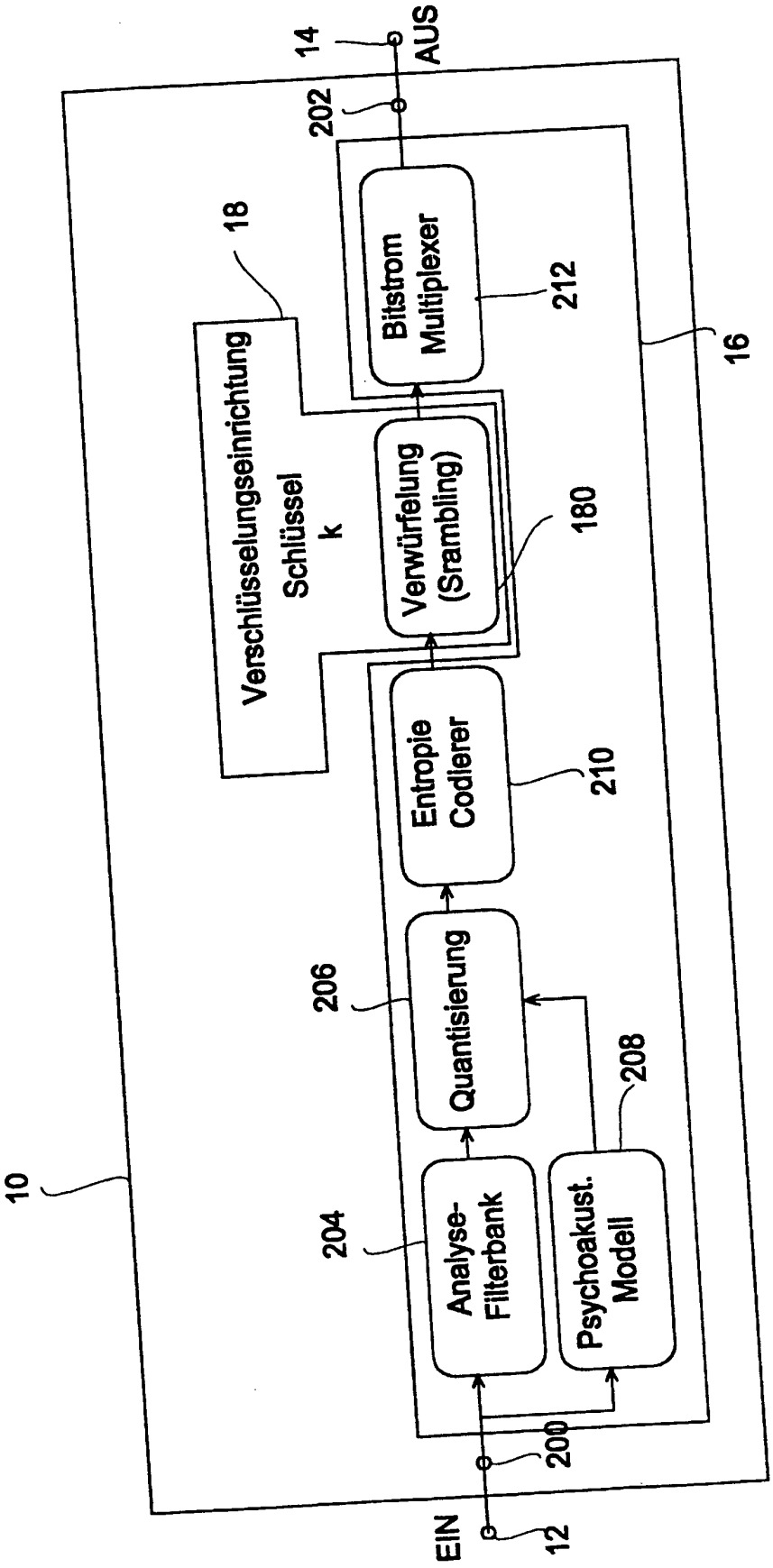

EIN
12
AUS
14
10
16
200
202
204
206
208
210
212
180
18
Analyse-Filterbank
Psychoakust. Modell
Quantisierung
Entropie Codierer
Verwürfelung (Sramibling)
Verschlüsselungseinrichtung
Schlüssel k
Bitstrom Multiplexer

Fig. 3

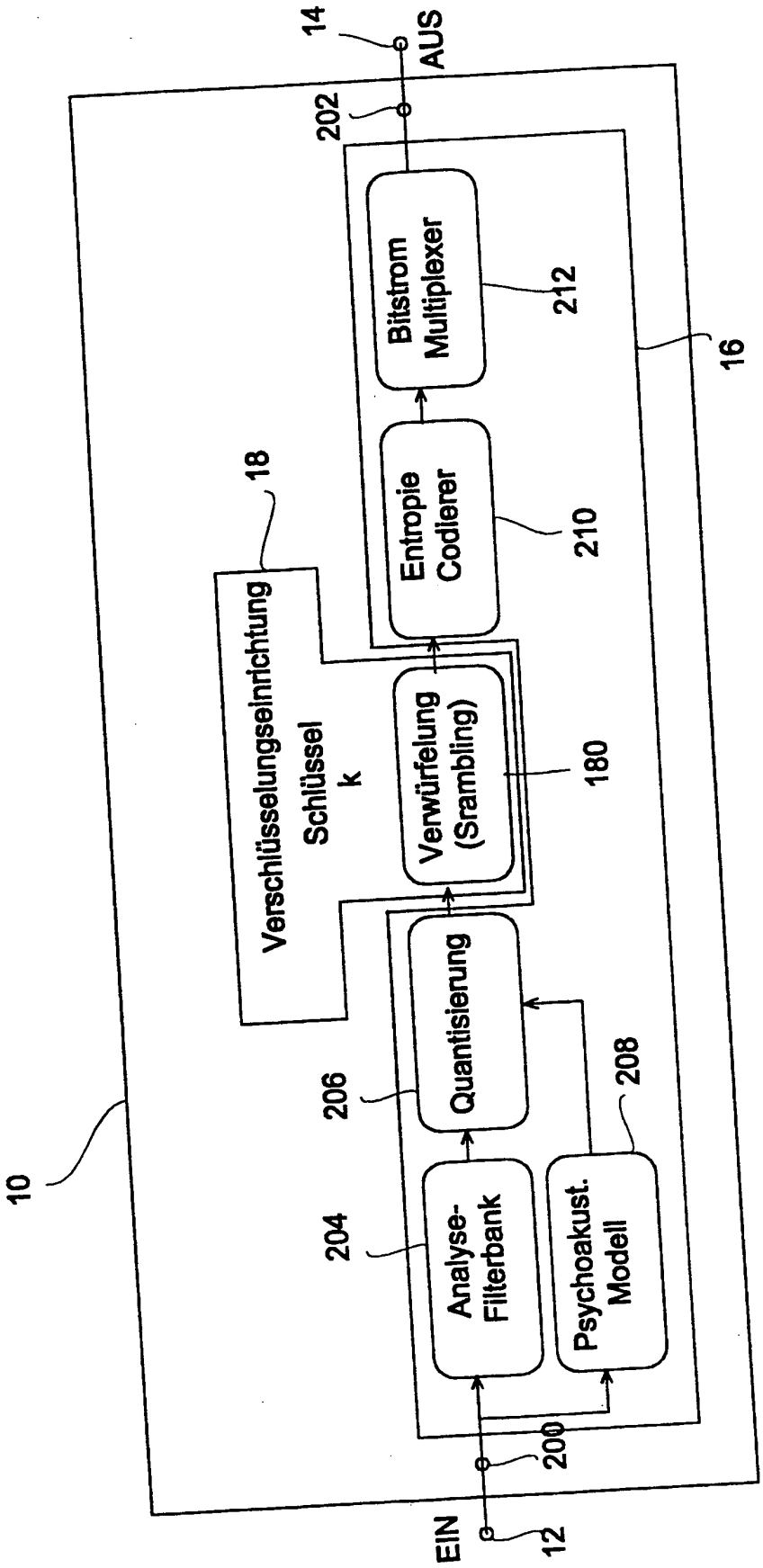

14
AUS
202
Bitstrom Multiplexer
212
16
18
Entropie Codierer
210
Verschlüsselungseinrichtung
Schlüssel k
Verwürfelung (Srambling)
180
Quantisierung
206
208
10
204
Analyse-Filterbank
Psychoakust. Modell
200
EIN
12

Fig. 4

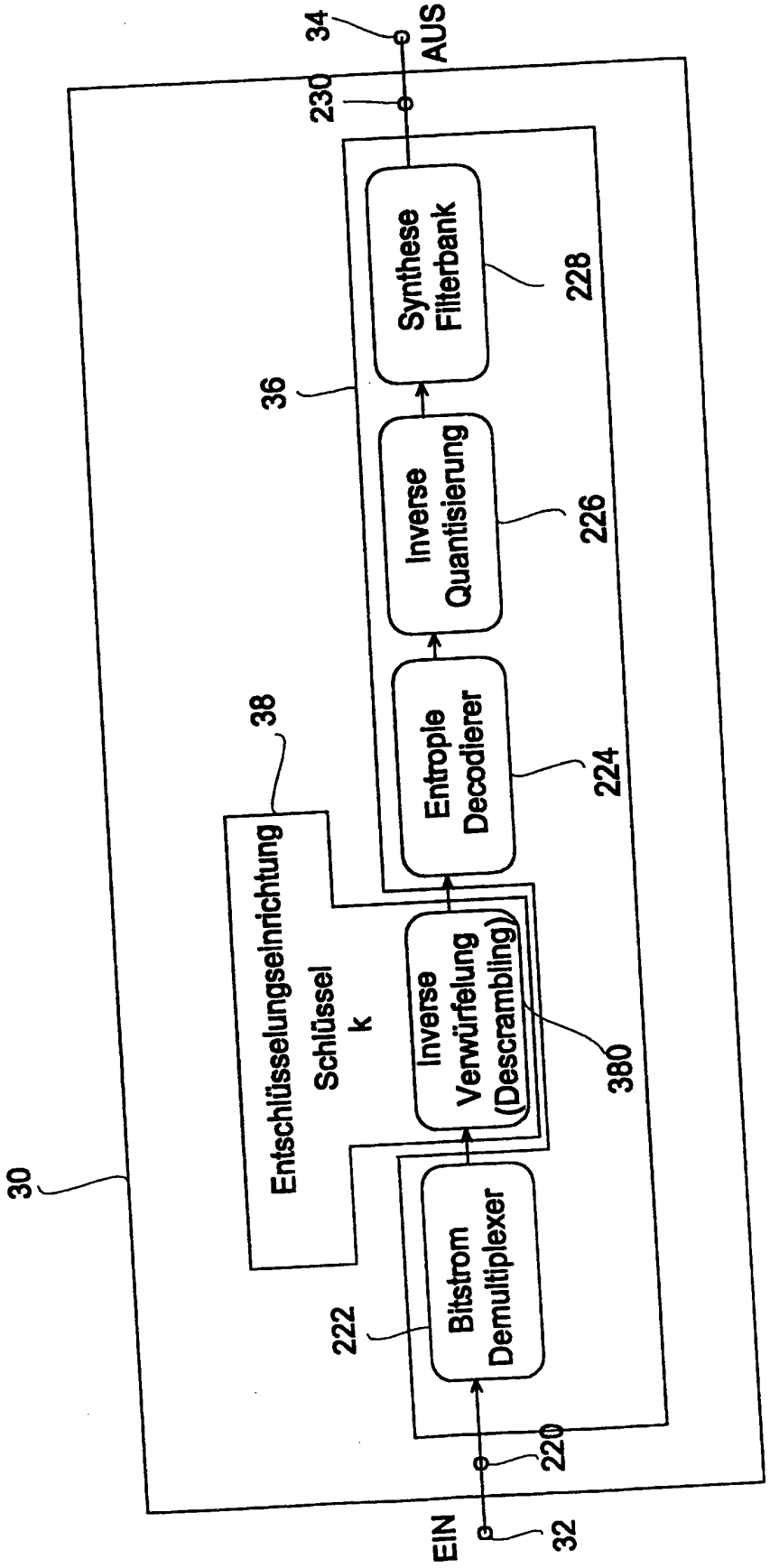

34
AUS
230
Synthese Filterbank
228
36
Inverse Quantisierung
226
38
Entroplo Decodierer
224
Entschlüsselungseinrichtung
Schlüssel
k
Inverse Verwürfelung (Descrambling)
380
30
222
Bitstrom Demultiplexer
220
EIN
32

Fig. 5

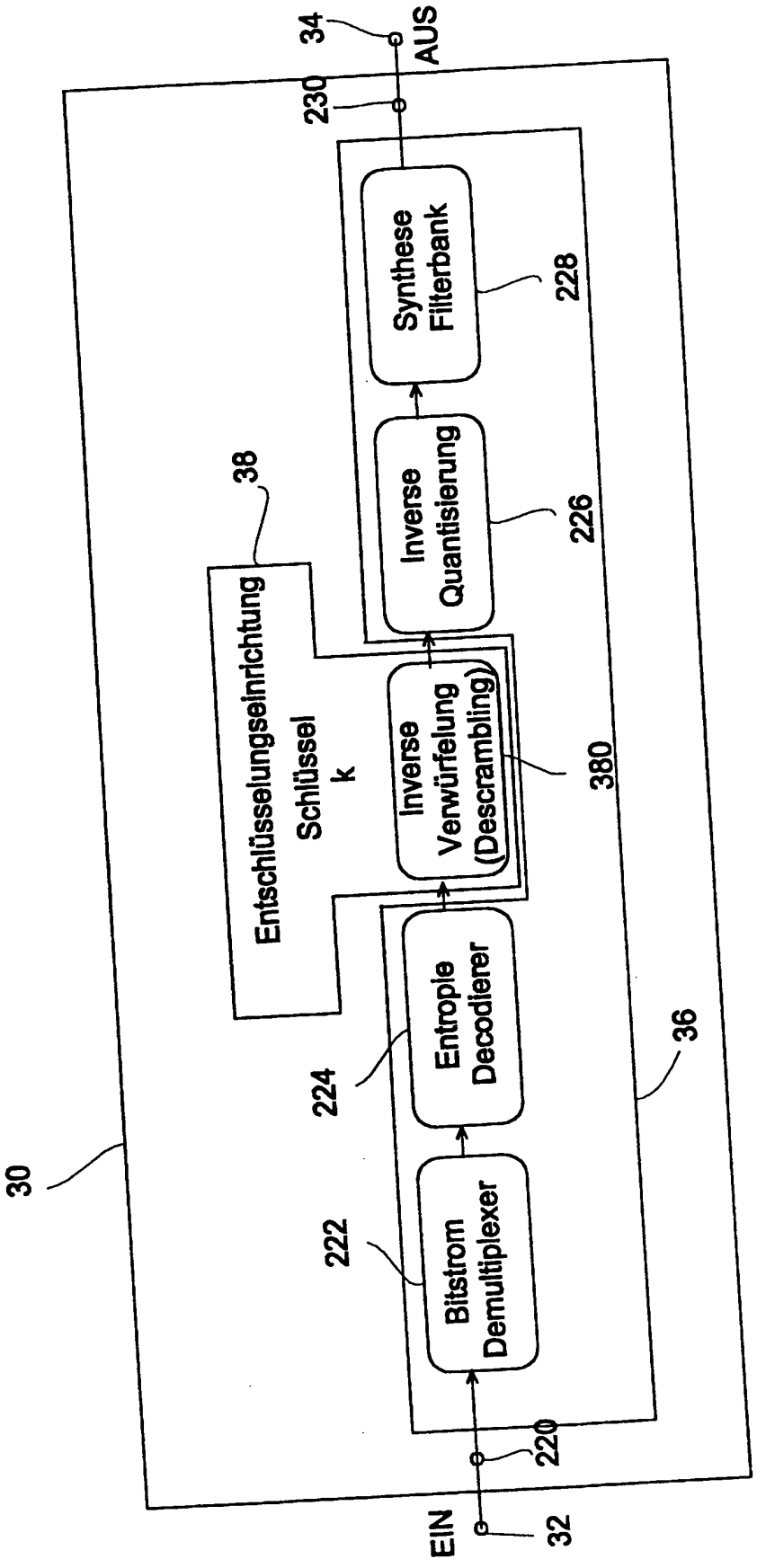

30
EIN
32
220
Bitstrom Demultiplexer
222
Entropie Decodierer
224
Entschlüsselungseinrichtung
Schlüssel k
38
Inverse Verwürfelung (Descrambling)
380
Inverse Quantisierung
226
Synthese Filterbank
228
230
AUS
34
36

Fig. 6

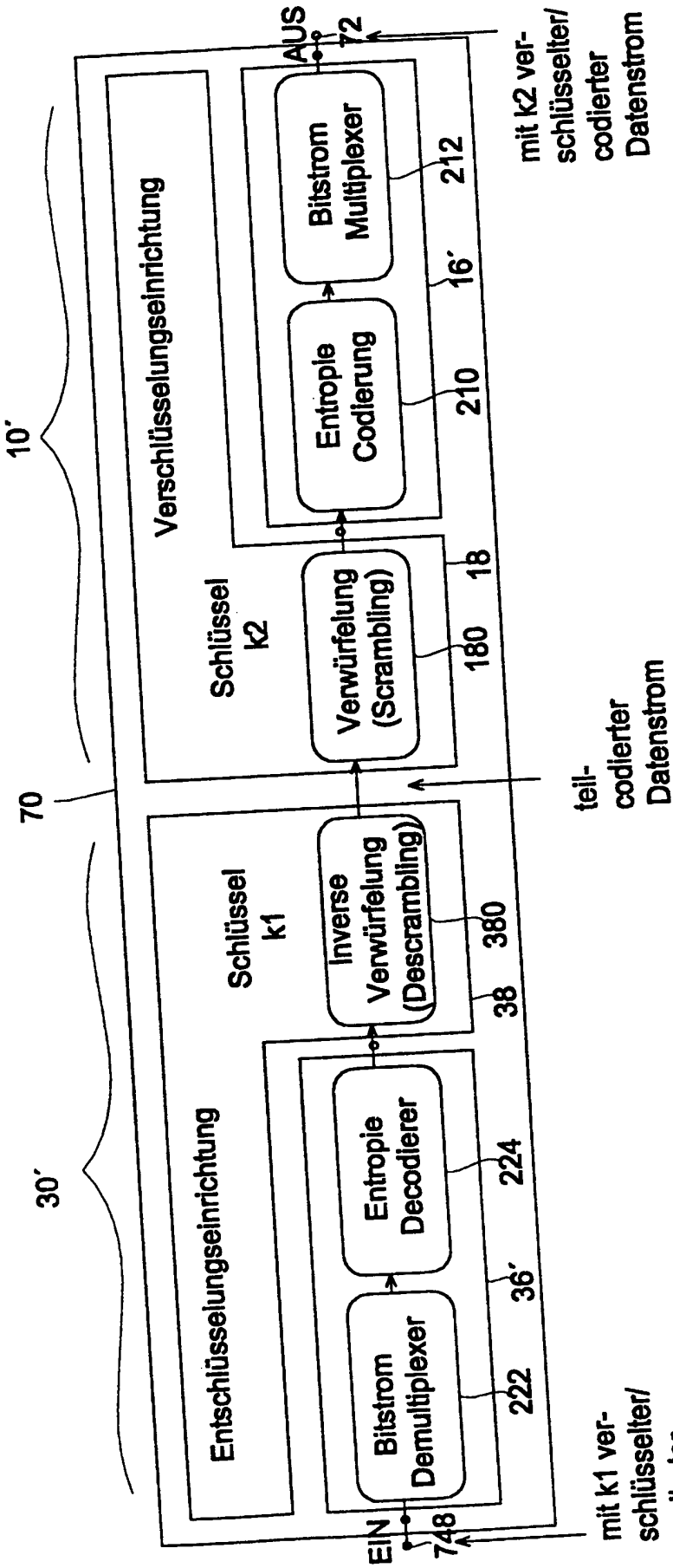

10'
30'
70
Verschlüsselungseinrichtung
Entschlüsselungseinrichtung
Schlüssel k2
Schlüssel k1
Bitstrom Multiplexer
Entropie Codierung
Verwürfelung (Scrambling)
Inverse Verwürfelung (Descrambling)
Entropie Decodierer
Bitstrom Demultiplexer
AUS
EIN
72
748
212
210
16'
18
180
380
38
224
36'
222
mit k2 verschlüsselter/ codierter Datenstrom
teil- codierter Datenstrom
mit k1 verschlüsselter/ codierter Datenstrom

Fig. 7

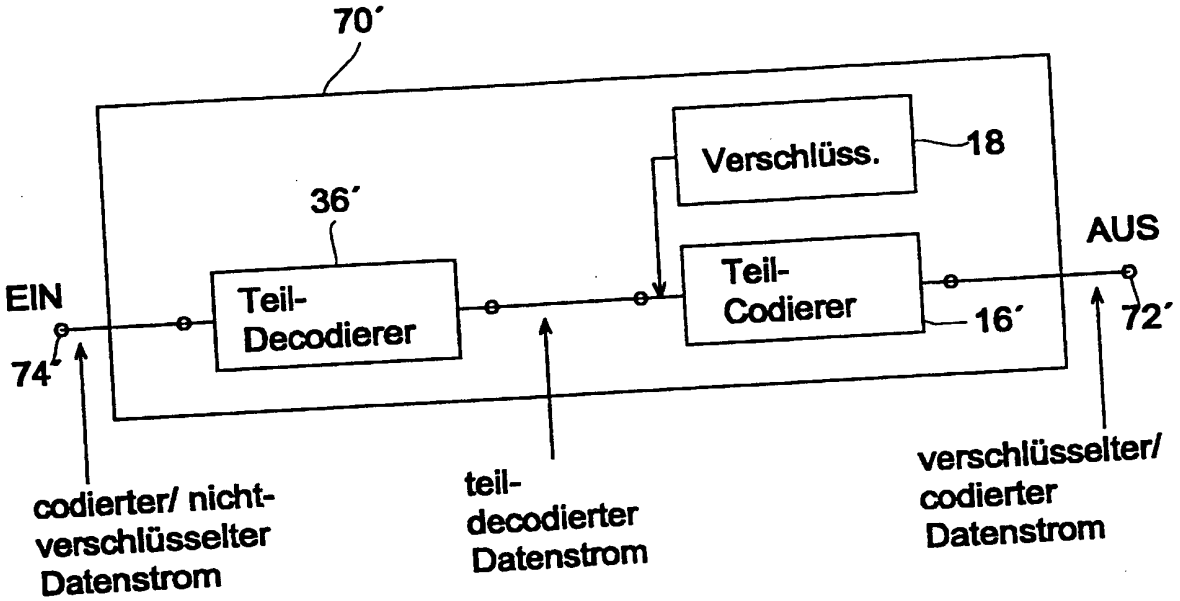

70´
Verschlüss.
18
36´
AUS
EIN
Teil-
Decodierer
Teil-
Codierer
16´
72´
74´
codierter/ nicht-
verschlüsselter
Datenstrom
teil-
decodierter
Datenstrom
verschlüsselter/
codierter
Datenstrom

Fig. 8

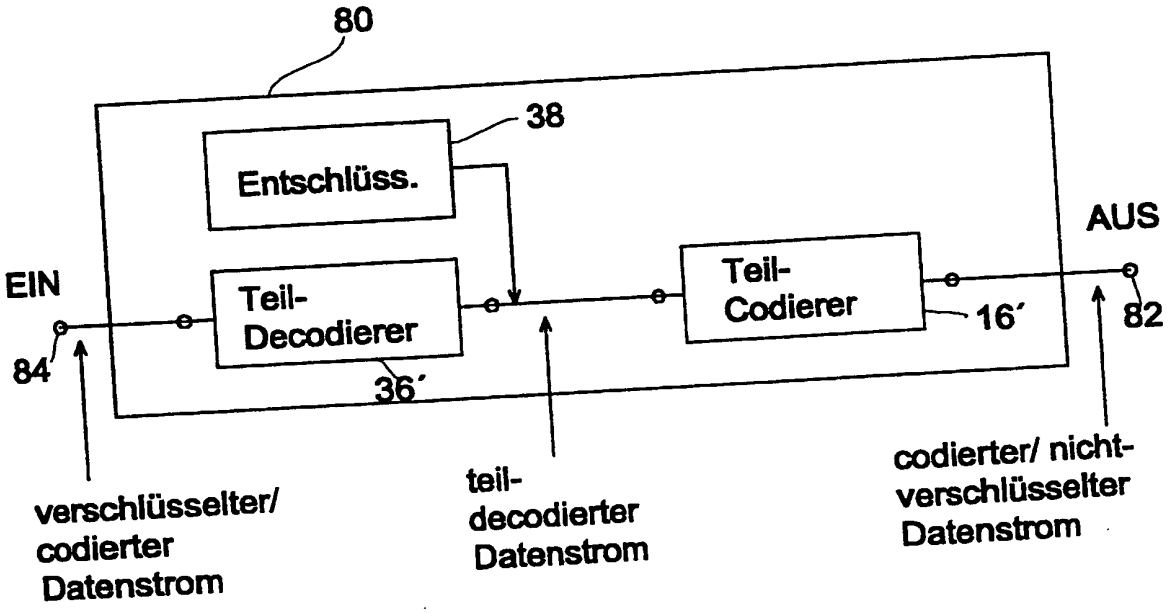

80
38
Entschlüss.
AUS
EIN
Teil-
Decodierer
Teil-
Codierer
16´
82
84´
36´
verschlüsselter/
codierter
Datenstrom
teil-
decodierter
Datenstrom
codierter/ nicht-
verschlüsselter
Datenstrom

Fig. 9

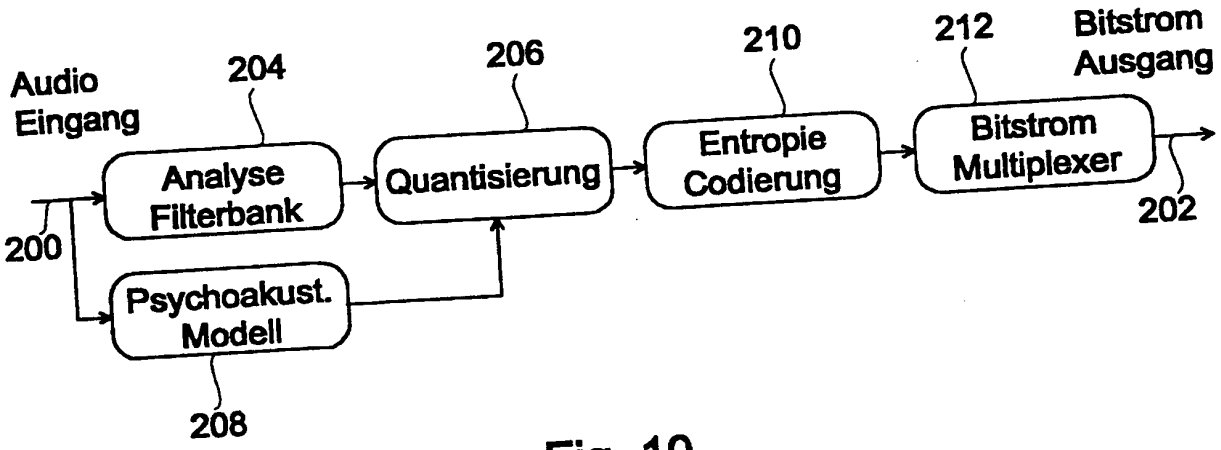

Audio
Eingang
204
206
210
212
Bitstrom
Ausgang
Analyse
Filterbank
Quantisierung
Entropie
Codierung
Bitstrom
Multiplexer
200
202
Psychoakust.
Modell
208

Fig. 10

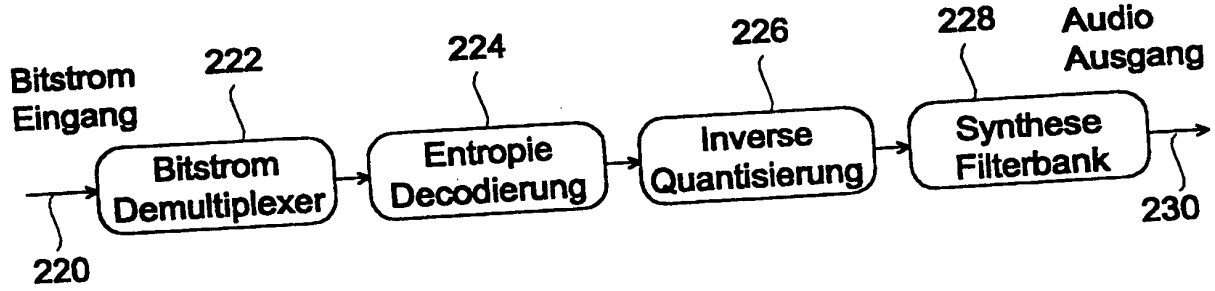

Bitstrom
Eingang
222
224
226
228
Audio
Ausgang
Bitstrom
Demultiplexer
Entropie
Decodierung
Inverse
Quantisierung
Synthese
Filterbank
220
230

Fig. 11

INTERNATIONAL SEARCH REPORT

Inter[illegible] Application No
PCT/EP 99/09978

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04K1/00 H04N7/167 H04N7/26

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04K H04N G10L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 636 279 A (AKIYAMA TOSHIHIDE ET AL) 3 June 1997 (1997-06-03) abstract column 1, line 58 -column 3, line 28; claims 1-11; figure 8 ---	1-4, 23-30
Y		5-14,16
Y	QUACKENBUSH ET AL.: "Noiseless Coding of Quantized Spectral Components in MPEG-2 Advanced Audio Coding" 1997 IEEE ASSP WORKSHOP ON APPLICATIONS OF SIGNAL PROCESSING TO AUDIO AND ACOUSTICS, 19 October 1997 (1997-10-19), XP002135840 cited in the application the whole document --- -/--	5-14,16, 20-22

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
17 April 2000	08/05/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Foglia, P

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP 99/09978

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y A	US 5 208 857 A (LEBRAT FRANCOIS) 4 May 1993 (1993-05-04) abstract column 2, line 26 -column 3, line 5; claims 2,4; figures 2,4-6	1-4,15, 23-30 7 5,6
Y	WO 98 21852 A (SCIENTIFIC ATLANTA) 22 May 1998 (1998-05-22) abstract page 8, line 12 -page 13, line 23; figures 6-8	17-22
Y	EP 0 805 592 A (INTEL CORP) 5 November 1997 (1997-11-05) abstract column 6, line 31 -column 8, line 29; claims; figures 3-5	17-22
P,X	EP 0 920 209 A (THOMSON MULTIMEDIA SA) 2 June 1999 (1999-06-02) paragraph '0004! - paragraph '0009! paragraph '0024! - paragraph '0039!	1-4,15, 23-30

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/EP 99/09978

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5636279 A	03-06-1997	JP 6069916 A	11-03-1994
		JP 6090451 A	29-03-1994
		JP 6303608 A	28-10-1994
		JP 6303609 A	28-10-1994
		CN 1085724 A,B	20-04-1994
		CN 1208292 A	17-02-1999
		CN 1208293 A	17-02-1999
		DE 69324077 D	29-04-1999
		DE 69324077 T	18-11-1999
		DE 69327675 D	24-02-2000
		EP 0582122 A	09-02-1994
		EP 0778705 A	11-06-1997
		EP 0888008 A	30-12-1998
		KR 9710045 B	20-06-1997
		US 5377266 A	27-12-1994
US 5208857 A	04-05-1993	FR 2661585 A	31-10-1991
		DE 69106033 D	02-02-1995
		DE 69106033 T	29-06-1995
		EP 0454556 A	30-10-1991
WO 9821852 A	22-05-1998	US 5937067 A	10-08-1999
		AU 7182398 A	03-06-1998
EP 0805592 A	05-11-1997	AU 2748597 A	26-11-1997
		CA 2204219 A	03-11-1997
		JP 10074364 A	17-03-1998
		WO 9742593 A	13-11-1997
EP 0920209 A	02-06-1999	FR 2771581 A	28-05-1999
		JP 11225323 A	17-08-1999

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP 99/09978

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 H04K1/00 H04N7/167 H04N7/26

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 H04K H04N G10L

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	US 5 636 279 A (AKIYAMA TOSHIHIDE ET AL) 3. Juni 1997 (1997-06-03) Zusammenfassung	1-4, 23-30
Y	Spalte 1, Zeile 58 -Spalte 3, Zeile 28; Ansprüche 1-11; Abbildung 8 ---	5-14,16
Y	QUACKENBUSH ET AL.: "Noiseless Coding of Quantized Spectral Components in MPEG-2 Advanced Audio Coding" 1997 IEEE ASSP WORKSHOP ON APPLICATIONS OF SIGNAL PROCESSING TO AUDIO AND ACOUSTICS, 19. Oktober 1997 (1997-10-19), XP002135840 in der Anmeldung erwähnt das ganze Dokument --- -/--	5-14,16, 20-22

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

[X] Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :

"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist

"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)

"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht

"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden

"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist

"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
17. April 2000	08/05/2000

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Foglia, P

Formblatt PCT/ISA/210 (Blatt 2) (Juli 1992)

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP 99/09978

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X Y A	US 5 208 857 A (LEBRAT FRANCOIS) 4. Mai 1993 (1993-05-04) Zusammenfassung Spalte 2, Zeile 26 -Spalte 3, Zeile 5; Ansprüche 2,4; Abbildungen 2,4-6	1-4,15, 23-30 7 5,6
Y	WO 98 21852 A (SCIENTIFIC ATLANTA) 22. Mai 1998 (1998-05-22) Zusammenfassung Seite 8, Zeile 12 -Seite 13, Zeile 23; Abbildungen 6-8	17-22
Y	EP 0 805 592 A (INTEL CORP) 5. November 1997 (1997-11-05) Zusammenfassung Spalte 6, Zeile 31 -Spalte 8, Zeile 29; Ansprüche; Abbildungen 3-5	17-22
P,X	EP 0 920 209 A (THOMSON MULTIMEDIA SA) 2. Juni 1999 (1999-06-02) Absatz '0004! - Absatz '0009! Absatz '0024! - Absatz '0039!	1-4,15, 23-30

Formblatt PCT/ISA/210 (Fortsetzung von Blatt 2) (Juli 1992)

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Inter. [illegible]les Aktenzeichen
PCT/EP 99/09978

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
US 5636279 A	03-06-1997	JP 6069916 A	11-03-1994
		JP 6090451 A	29-03-1994
		JP 6303608 A	28-10-1994
		JP 6303609 A	28-10-1994
		CN 1085724 A,B	20-04-1994
		CN 1208292 A	17-02-1999
		CN 1208293 A	17-02-1999
		DE 69324077 D	29-04-1999
		DE 69324077 T	18-11-1999
		DE 69327675 D	24-02-2000
		EP 0582122 A	09-02-1994
		EP 0778705 A	11-06-1997
		EP 0888008 A	30-12-1998
		KR 9710045 B	20-06-1997
		US 5377266 A	27-12-1994
US 5208857 A	04-05-1993	FR 2661585 A	31-10-1991
		DE 69106033 D	02-02-1995
		DE 69106033 T	29-06-1995
		EP 0454556 A	30-10-1991
WO 9821852 A	22-05-1998	US 5937067 A	10-08-1999
		AU 7182398 A	03-06-1998
EP 0805592 A	05-11-1997	AU 2748597 A	26-11-1997
		CA 2204219 A	03-11-1997
		JP 10074364 A	17-03-1998
		WO 9742593 A	13-11-1997
EP 0920209 A	02-06-1999	FR 2771581 A	28-05-1999
		JP 11225323 A	17-08-1999